DIGITAL THREATS to *Democratic Elections:*

How Foreign Actors Use Digital Techniques to Undermine Democracy

Lead author: Chris Tenove
Co- authors: Jordan Buffie, Spencer McKay, David Moscrop
Project supervisors: Mark Warren and Max Cameron

DIGITAL THREATS TO DEMOCRATIC ELECTIONS:

How Foreign Actors Use Digital Techniques to Undermine Democracy

Lead author:

Chris Tenove, Postdoctoral Research Fellow,
Department of Political Science, University of British Columbia (UBC);

Co- authors:

Jordan Buffie, MA student, UBC Political Science
Spencer McKay, PhD Candidate, UBC Political Science
David Moscrop, Postdoctoral Researcher, Simon Fraser University

Project supervisors:

Mark Warren, Professor and Merilees Chair in the Study of Democracy, UBC Political Science
Max Cameron, Professor and Director of the Centre for the Study of Democratic Institutions, UBC Political Science

CENTRE FOR THE STUDY OF DEMOCRATIC INSTITUTIONS
The University of British Columbia

ABOUT THIS REPORT

This report provides a synthesis of current research on foreign actors' use of digital techniques to interfere in elections, with an emphasis on social science findings. The report was researched and written during the summer and fall of 2017, by researchers in the Department of Political Science at the University of British Columbia.

We would like to thank the Social Sciences and Humanities Research Council for a Knowledge Synthesis Grant to pursue this project. The project also received support from the Centre for the Study of Democratic Institutions (CSDI) and its Global Challenges to Democracy cluster (supported by UBC's office of the Vice-President Research + Innovation at UBC), and from SSHRC grant #435-2016-1368, held by Professor Richard Johnston.

The authors are grateful for in-depth discussions with several individuals, including David Ascher, Alexandra Samuel, and Phillip Smith, as well as UBC professors Paul Quirk, Taylor Owen, Lisa Sundstrom, and Heidi Tworek. Chris Tenove presented a portion of this report at the American Political Science Association annual conference in San Francisco (August 2017), and is grateful in particular for comments by Jennifer Forestal. The authors remain responsible for any errors or omissions.

Thank you as well for assistance from Rebecca Monnerat at CSDI, and to Oliver McPartlin for help with this report's design and layout.

Please send all questions and feedback regarding this report to: cjtenove@mail.ubc.ca.

Report completion: November, 2017

Report publication: January, 2018

Social Sciences and Humanities Research Council of Canada | Conseil de recherches en sciences humaines du Canada | Canada

This research was supported by the Social Sciences and Humanities Research Council of Canada.

TABLE OF CONTENTS

Executive Summary 1

Introduction 4

Approach and Methodology 7

What is Threatened? Key Democratic Functions in Elections 8

Threats that Foreign Actors Pose to Self-Determination 11

Four Techniques of Digital Interference in Elections 12

Cyber Attacks on Systems and Databases 12

Timeline of Digital Interference in Elections 13

Digital Misinformation: Fake News and Computational Propaganda 16

Manipulating Preferences via Big Data and Micro-targeting 19

Internet Trolling 22

What Are the Impacts of These Threats? 26

What Threat Actors Exist, with what Intentions and Capabilities? 33

What Are the Key Vulnerabilities to Digital Threats and What Counter-measures Can Be Taken? 36

Deficits in Digital Literacy and Data Protection 36

Polarization and Hyper-partisanship in Political Cultures and Media Systems 38

Social Media Design and Policies 40

Weak Regulatory and Enforcement Capacities of States 43

Absence of clear international norms and laws on cyber interference 47

Research and Knowledge Gaps 50

Conclusion 52

Works Cited 53

EXECUTIVE SUMMARY

This report addresses key questions about foreign actors' use of digital communication technologies (DCTs) to interfere in democratic elections. It does so by employing the schema of a cyber-security "threat model." A threat model asks the following key questions: What in a system is most valued and needs to be secured? What actions could adversaries take to harm a system? Who are potential adversaries, with what capacities and intentions? What are the system's key vulnerabilities? What will be the most effective counter-measures to address these threats? The authors of this report draw on existing research to engage these questions. Several key observations are:

The threat of digital interference is not limited to its impact on electoral outcomes.

Foreign actors can use digital techniques to undermine three critical elements of democratic elections: *fair opportunities for citizen participation* (such as voting, running for office, or contributing to public debates); *public deliberation* that enables citizens to share and understand each other's insights and perspectives; and key *institutional actions* by electoral commissions, political parties, and other organizations, including the enforcement of electoral regulations.

Foreign actors can use four principal techniques to interfere in elections.

This report examines four techniques that figure prominently in accounts of foreign interference. *Hacking attacks* target systems, accounts and databases, with the aim of accessing, changing or leaking private information. *Mass misinformation and propaganda campaigns* promote false, deceptive, biased and inflammatory messages, often using bots or fake social media accounts. Foreign actors acquire data about populations or individuals to develop messages for *micro-targeted manipulation*. Finally, foreign actors mount *online "trolling" operations* to threaten, stigmatize, and harass individuals or groups.

Evidence shows that these techniques can undermine democratic participation, deliberation, and institutional action, but the extent of their impact remains unclear.

More research is needed to specify the downstream effects of digital interference. For instance, it is not yet clear whether foreign actors using digital techniques have actually flipped elections.

However, there is clear evidence that digital techniques can undermine *participation,* and do so in ways that may particularly affect groups that already struggle for equal political participation. For instance, troll networks frequently target women and minority groups with threatening and stigmatizing messages. There is also extensive evidence that foreign actors use DCTs in ways that degrade *public deliberation*, such as by promoting "fake news" and undermining norms of inclusivity, respect, and trust. Finally, foreign actors use digital techniques to breach voting systems, violate campaign laws and regulations, and otherwise undermine key *institutional actions* required for fair elections.

States and non-state actors use these techniques, often in 'partnership' with domestic actors.

Digital techniques for election interference are widely used by non-state actors, including terrorist groups, hacktivists, and extremist social movements. State actors are particularly dangerous, however, as they have the human and financial resources to use these techniques at large-scale, as seen in Russia's interference in the 2016 US elections.

While foreign actors sometimes promote particular candidates, policies or ideologies, they may also seek to undermine government legitimacy, exacerbate social discord, or erode citizens' trust in democratic institutions and each other.

Foreign actors are not alone in using these digital techniques to undermine democracy. Domestic actors use similar techniques. They may also act as de facto "partners" in foreign interference operations, such as when domestic politicians and media outlets promote the deceptive, polarizing, and propagandistic messages of foreign actors.

Foreign actors interfere in elections by exploiting states' systemic and institutional vulnerabilities.

Key vulnerabilities are deficits in citizens' *digital literacy and data protection*; shortcomings

in the *design and policies of social media platforms*; high levels of *polarization in political cultures and media systems*; and inadequate *electoral regulation* given today's digital realities.

There is also an *international dimension* of vulnerability, as current international laws and norms do not adequately address cyber-attacks and information operations.

States differ in the degree to which they possess these vulnerabilities and thus differ in their susceptibility to different forms of interference.

There are many possible counter-measures to digital interference but no proven solutions.

Responses to digital interference include digital literacy training for citizens, design and policy changes by social media platforms, new forms of state electoral and criminal regulation, and new international laws on cyber interference. While these and other actions are being pursued, we lack clear evidence about what will work.

Many knowledge gaps need to be addressed.

The problem of digital interference in elections has only recently begun to receive serious research attention. This report reveals many gaps in knowledge. For instance, we lack strong findings on the short-term or long-term harms that digital techniques may do to democratic institutions and norms, and we lack good cross-national comparisons of state vulnerabilities to interference. Critically, there is little clarity on the policy measures that Canada or other democratic countries should take to effectively address digital threats to elections. Research and policy experimentation are greatly needed.

INTRODUCTION

Our democracy is under digital attack. That concern is now raised before and after every major election. Newspaper headlines and social media feeds are full of stories of hacked documents, foreign troll networks, and bot-driven misinformation campaigns. Foreign actors, from states to extremist social movements to corporations, use these digital techniques to influence election outcomes or to weaken democratic systems.

Attention to this issue has increased dramatically due to interference in the 2016 US election. Referring to Russian cyber-interference in that election, former Central Intelligence Agency Acting Director Michael Moore stated: "It is an attack on our very democracy. It's an attack on who we are as a people... this is to me not an over-statement, this is the political equivalent of 9/11" (Morell and Kelly 2016).

Interference in elections using digital communication technologies (DCTs) did not begin or end in 2016, however. There is evidence of cyber attacks and computer-driven propaganda in Argentina, Brazil, France, Germany, Philippines, the United Kingdom (UK), and many other countries (for overviews, see Bradshaw and Howard 2017; Communications Security Establishment 2017; Woolley and Howard 2017). These and other accounts of digital interference in elections have raised serious concerns among researchers, policymakers and citizens about the quality and legitimacy of democratic politics.

To better understand the threats of digital interference to democratic elections, this report uses the schema of the cyber-security "threat model." A threat model includes the following key questions: What in a system is most valued and needs to be secured? What actions could potential adversaries take to harm a system? Who are potential adversaries, with what capacities and intentions? What are the key vulnerabilities of the system? What are the most important counter-measures to take to address these threats? This report assesses the current state of research on these questions and identifies important gaps in knowledge.

BACKGROUND: NEW COMMUNICATION TECHNOLOGIES, NEW DEMOCRATIC PRACTICES

Novel threats to democracy have arisen in a context of changing democratic practices. It is widely recognized that the form and quality of democratic politics are highly dependent on societies' communication technologies (Cameron 2013; Habermas 1991). As DCTs have evolved in the last three decades, so too has debate about their impact on democracy. Earlier scholarship highlighted opportunities for more open and participatory "e-democracy" and "e-government" (Hague and Loader 1999), though practical difficulties became clear (Chadwick 2006; Margolis and Moreno-Riaño 2009). More recently, social media have become fundamental "spaces" for political organizing and activity, and people in some countries get much of their information on public matters from social media sites (Messing and Westwood 2014; Silverman 2016).

Scholarship on elections and DCTs has often focused on the use of new digital techniques in campaigns. Political parties and other political actors increasingly use data analytics, digital media, and micro-targeting, which make campaigns more "personalized" (Chadwick and Stromer-Galley 2016; Hersh 2015; Kreiss 2016). . There is also clear evidence that voter turnout can be altered by social pressure mobilized on Facebook (Bond et al. 2012), While much of this literature focuses on campaigning in the US, cross-national studies show that DCTs may be used in similar ways but can have different consequences on electoral outcomes or citizen engagement due to institutional, social and cultural differences (Anduiza, Jensen, and Jorba 2012; Vaccari 2013).

Scholars have also shown that social media can be effectively used by civil society organizations and social movements to mobilize quickly, with little organizational structure, and with more turbulent and unpredictable results (Bennett and Segerberg 2013; Earl and Kimport 2011; Karpf 2012; Margetts et al. 2015). The Arab Spring uprisings may have been the period of peak enthusiasm for DCTs to be used as a kind of "liberation technology" to promote democracy and liberal rights (Diamond 2010). Social media are seen as a necessary but insufficient factor in these uprisings (Howard and Hussain 2013), and social media use may serve as an obstacle to *transitions* to democracy after revolutions (Lynch, Freelon, and Aday 2016). Authoritarian regimes increasingly used

DCTs to suppress dissent, threaten both domestic and foreign activists and political opponents, and consolidate power over their populations (Deibert et al. 2010; Deibert 2015; Gunitsky 2015; G. King, Pan, and Roberts 2017).

Changes in communication technologies have also disrupted international politics. There are intense debates in international law and international relations regarding state sovereignty and interstate conflict in cyberspace (Buchanan 2017; Nicholas Tsagourias 2015). The United Nations Group of Governmental Experts stated that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory" (United Nations General Assembly 2013). However, this position has not been developed into clear and enforceable norms or treaties, and international progress on the matter appears to be stalled (Segal 2017). Legal scholars who examine the narrower issue of election interference by foreign actors using DCTs argue that that there are major gaps in international norms and laws to address the issue (Crootof 2018; Ohlin 2017; Shackelford et al. 2017).

APPROACH AND METHODOLOGY

To synthesize the state of knowledge on foreign digital interference in elections, we pursued a critical interpretive synthesis (Dixon-Woods et al. 2006; Perski et al. 2017). Conventional literature reviews and synthesis projects in the social sciences primarily seek to aggregate existing findings, which is possible when there are stable concepts in a field that have been tested using comparable methods. However, on a novel topic such as the one examined by this report, greater induction and interpretation of existing literature is required. Specifically, it is necessary to develop a *synthesizing argument* that "integrates evidence from across the studies in the review into a coherent theoretical framework, [whose] function is to provide more insightful, formalised, and generalisable ways of understanding a phenomenon" (Dixon-Woods et al. 2006, 39). The synthesizing argument we use is the cyber-security "threat model." This entailed conceptual work to identify key normative functions of democratic elections, which we used to integrate evidence on the techniques, actors, and systemic vulnerabilities that generate threats to these functions.

This report draws on peer-reviewed academic research and on "grey literature," including governmental and non-governmental reports, non-peer-reviewed studies by academic researchers, and high-quality works of journalism and commentary. An emphasis on grey literature was essential since pivotal cases of electoral interference and important technological, social and policy changes have occurred in the last two years. Our initial scoping review in May 2017 revealed very little peer-reviewed material on electoral interference via hacking, social media propaganda, and other cyber techniques. Two genres of grey literature proved particularly useful. One is working papers by scholars that are published by academic research centres, such as the Oxford Internet Institute at the University of Oxford, and the Citizen Lab of the University of Toronto. A second genre is investigative journalism by academics (e.g. Rid 2016) and by journalists using high-quality qualitative and quantitative research methods (Silverman 2016; Silverman et al. 2017).

Research in this area is quickly expanding, and we expect significant growth in peer-reviewed literature to address some of the current shortcomings and gaps.

WHAT IS THREATENED?
KEY DEMOCRATIC FUNCTIONS IN ELECTIONS

Democratic elections are more than what happens in the voting booth. Drawing primarily on democratic theory, this section proposes a framework for identifying important normative "functions" that should be advanced during election periods, and which may be undermined by the digital techniques discussed in this report.

There are many competing understandings of democracy and the role of elections. Rather than seek to resolve which "model of democracy" to follow, some contemporary democratic theorists have identified key *normative functions* that political systems need to achieve to count as democratic (Mansbridge et al. 2012; Warren 2017). Following Warren (2017, 43–45), we focus on three functions: 1) the empowered inclusion of all members of a demos via votes, voices, legal challenges, political mobilization, and other means; 2) processes of collective will formation that help organize competing claims into agendas and understandings that can ground legitimate collective action; and 3) formal and informal institutions that facilitate effective and legitimate collective action. For the purposes of this report, these three functions will be described as *Participation, Public Deliberation,* and *Institutional Action.*

If these three democratic functions are advanced during elections, citizens are more likely to enjoy a range of important democratic principles and goods. For instance, the *autonomy* of citizens is protected when they have opportunities to understand their own interests and values, and when they have sufficient powers of inclusion to advance these interests and values by running for office, voting, and contributing to public debates (Dahl 1989, Ch. 7). The *equality* of citizens is bolstered if they have similar opportunities for inclusion, but also if processes of collective will formation and action treat people with equal moral respect (Young 2000). Good public deliberation will advance the *epistemic quality* of debate and decision-making (Estlund 2009), the capacity for publics to identify and respond to *shared problems* (Dewey 1991), and people's *trust* in their political institutions (Warren 1999). If institutions can ensure fair voting and enforce electoral regulations, political systems will tend to have greater capacity for *non-violent* contests for power and changes in government (Przeworski 1999). As different digital techniques target functions of democracy, they may threaten these and other democratic goods.

1. Participation

Democracy is, most basically, *rule by the people*. Election periods are an important time for people to influence the governments and policies that rule them. To do so, people require universal and equal adult suffrage, opportunities to stand for office, access to information about candidates and political processes, and the ability to engage in public discussions in formal and informal settings (Dahl 1989). These powers and opportunities give citizens a "place at the table" in political debates and decisions that affect them (Warren 2017, 48). To take advantage of these opportunities for participation, people also require protection from coercion and threat; recognition as valued members of their political community, and the cognitive or practical capacities to pursue their relevant interests and values.

Just as citizen *participation* in elections is multi-dimensional, so too are the threats to participation detailed in this report. These threats are problematic when they affect citizens in general. When they affect certain social groups disproportionately, they undermine the democratic principles of equality and equal moral respect. Digital interference in elections can have these effects. For instance, as this report discusses below, bots and troll networks frequently target members of social groups that already face challenges to full democratic participation, including women and visible minorities.

2. Public Deliberation

To continue the metaphor of the previous section, public deliberation is the process by which citizens with "seats at the table" in a democracy can exchange their views and reasons, and can thereby make collective, well-informed decisions. The periods of intense public communication before elections are therefore critical. Citizens need to put forward their concerns, insights, values, and interests; candidates must propose their platforms and respond to claims made by their opponents; and other domestic and foreign actors can weigh in with relevant views.

While ideal forms of public deliberation may never be achieved, social scientists continue to identify procedures and principles to make decision-making more deliberative. Citizens can engage in public deliberation in a very wide variety of contexts, from "everyday talk" among neighbours and co-workers, to newspaper opinion pages, to candidate debates and town hall discussions (Dewey 1991; Mansbridge et al. 2012). People can better connect their individual views to public debate when deliberation is guided by principles such as inclusivity or openness to diverse views, a commitment to reasonable and epistemically

valid claims, and an assumption of moral equality (Habermas 1990; Mansbridge et al. 2012; Young 2000).

Public deliberation can be harmed through practices that circulate false information and, more fundamentally, that undermine the possibility for people to have good discussions about what is true or false, valuable or harmful, acceptable or inappropriate.

This paper shows that foreign actors can use DCTs to push false or misleading information, or can suppress and filter information flows, in ways that undermine the epistemic validity of public deliberation. Foreign actors can also target social media platforms and other media organizations with polarizing and demeaning messages, which can corrode norms of inclusivity and respect. Through these and other means, foreign actors can threaten the processes by which citizens come to understand their shared problems and to pursue legitimate collective solutions.

3. Institutional Action and Electoral Regulation

Democracies not only require individual participation and collective talk, they must also take collective action—including the selection of representatives in elections. Institutions are needed to make collective decisions and enforce collective rules. For instance, democratic states have electoral commissions and supporting state agencies that oversee voting processes and enforce legal regulations of campaign tactics, campaign funding, and fair access to broadcast media. Other state institutions protect civic and political rights that are necessary for political participation, such as freedom of expression and association.

Political parties are also key institutions during and between elections in many political systems, as they conduct and fund campaigns, hold public forums, solicit donations, propose shared policies, and mobilize supporters (Dalton and Wattenberg 2002). Other non-state institutions help ensure fair elections, such as civil society groups that promote voter participation or monitor elections.

Foreign actors use DCTs to block or hamper institutional actions necessary for elections, including electoral commissions, other state agencies, and non-state institutions. Examples include the hacking of databases of electoral authorities and political parties, and violations of regulations on financial and other support by foreign actors in campaigns.

THREATS THAT FOREIGN ACTORS POSE TO SELF-DETERMINATION

The digital techniques that this report examines, such as circulating misinformation or issuing online threats, are harmful to democracy even if pursued by domestic. These techniques may be more normatively problematic when used by *foreign* actors, however. Foreign interference using these techniques violates the democratic principle of *self-determination*, as outsiders seek to impose rules and rulers on the citizens who should establish them. Moreover, many of the techniques that we describe are violations of the rules for elections that democratic citizens and their governments have developed and adopted.

Not all foreign contributions to elections are problematic, however. As Canada's Standing Senate Committee on Legal and Constitutional Affairs notes, the aim of electoral regulations should not be "to silence any foreign commentary on our elections. Individuals must be free to express their opinions on political matters throughout the world" (2017, 4).

There is considerable debate in democratic theory on contributions that non-citizens should be able to make. Few theorists contend that non-resident foreigners deserve the opportunity to vote in domestic elections, but many acknowledge that foreigners can make communicative contributions to public debates (Fung 2013; Goodin 2007). These communicative contributions can address people's affected interests and contribute valuable viewpoints that enhance the epistemic robustness of public debates (Sen 2009, 380). The kinds of digital techniques examined in this paper – such as "misinformation" and "trolling" – do not meet these standards.

FOUR TECHNIQUES OF DIGITAL INTERFERENCE IN ELECTIONS

Studies have identified four prominent techniques of digital interference in elections: cyber attacks on systems and databases, misinformation campaigns, micro-targeted manipulation, and trolling. These techniques are distinct, though they are often used in tandem. The following sub-sections describe each technique and give examples of its use.

CYBER ATTACKS ON SYSTEMS AND DATABASES

The theft and publication of political actors' private data has become a familiar form of political action. Examples include the Snowden leaks about mass surveillance by the US and other states, leaks of Peruvian government communications that show extensive business influence, and leaks of the communications and contracts of surveillance technology companies (Coleman 2017). Leaked hacks have more recently been used to influence elections, most prominently in the leaked communications of the Democratic National Committee (DNC) in the 2016 US election and of Emmanuel Macron's campaign team in the 2017 French elections.

Not all hacked data is leaked. Indeed, experts suggest that governments and political parties regularly have their systems breached and data accessed – but not made public – as a regular part of state espionage practices (Banks 2016; Buchanan 2017).

Techniques

Being "hacked" means that an attacker gains access or control of digital devices, data servers, or digital services such as social media accounts. Cyber-security experts focus on threats to the confidentiality, integrity and availability of data (Andress 2011, 4–6). Copying and leaking data threatens its confidentiality; deleting or manipulating violates its integrity; and encryption or network disruption can change its availability.

Attackers break into systems and accounts in several ways. The most common is to trick people to give up account or system passwords, or to download and run malware,

often through deceptive emails and other messages. Attackers can also exploit software vulnerabilities in applications, devices, computers, or servers, and these exploits can be purchased on black markets.

One of the most profound threats to election integrity is the possibility of data breaches of voting machines, voter lists, or other databases and systems that are integral to the voting process itself. As will be discussed in the Impacts section, there is significant evidence that foreign actors have attempted to hack voting systems.

Attackers can also use information about their political opponents to influence campaigns. For instance, Andrés Sepúlveda, a hacker who confessed to assisting right-wing campaigns in Latin America, claims to have intercepted the communications of opponents in order to gain strategic advantages during campaigns (Robertson, Riley, and Willis 2016). Data breaches of the German parliament and other government agencies were believed to be part of Russian plans to interfere in the German elections (Stelzenmüller 2017).

Coleman (2017) proposes the term of the "public interest hack" to refer to "a computer infiltration for the purpose of leaking documents that will have political consequence." Coleman suggests that public interest hacks belong to two categories. The first category resembles traditional forms whistleblowing, such as the leak of the Pentagon Papers, which exposes wrongdoing to promote the public good. The second category includes leaks of material that are of interest *to* the public, but which may be pursued to advance the interests of the leaker

TIMELINE OF DIGITAL INTERFERENCE IN ELECTIONS

2014

UKRAINE

Attackers compromise computer systems of Ukraine's electoral authority. Allegedly by Russia.

US

Russia-based trolls promote fake story about chemical plant explosion in Louisiana, a test run for "fake news" strategy in 2016 election.

2015

APR–MAY

GERMANY

Cyberattack on German federal legislature compromises thousands of accounts, steals data. Allegedly by Russia.

US

Attackers gain access to communication system of Democratic National Committee (DNC).

2016

JUN

UK

Micro-targeting of voters in Brexit referendum to promote Leave position. Foreign role possibly violates election laws.

CONT'D P. 14

and not necessarily the interests *of* the public. An example of the former is the Panama Papers, an example of the latter is the "Guardians of Peace" hack of Sony Pictures (believed to be a retaliation by North Korea to Sony's release of the move *The Interview*). We propose that this second category be called "strategic hacks" rather than public interest hacks. Actors conduct strategic hacks advance their own aims, and do not acquire, manage, or publicize information in ways that can maximize public benefit.

The apparent truth value of hacked data is very high, as it can include the kinds of substantive, internal documents that are usually only available to police, intelligence agencies, or through disclosure in judicial processes. In addition, hacked data and communications are often assumed to be more genuine because they have not been crafted for public scrutiny (Sauter 2017).

However, it has been shown that actors sometimes release altered data. Researchers from the University of Toronto's Citizen Lab (2017) call these "tainted leaks," which they define as "the deliberate seeding of false information within a larger set of authentically stolen data." They show how critics of the Russian government have had their communications hacked and leaked, but with modifications made to the communications in order to further discredit opponents of the Russia government. A similar strategy was used in the leak of communications of the Macron campaign during the French election (BBC 2017).

JUN–JUL

UK

Leak of hacked DNC emails, by DCLeaks and then Wikileaks

AUG

US

Department of Homeland Security (DHS) reports attacks on election systems in Arizona and Illinois. DHS will later announce that systems of 21 states were attacked.

OCT

US

Emails of Jon Podesta, Hilary Clinton campaign chair, are leaked. Begins hours after release of video of Trump's pussy-grabbing comment.

OCT

US

DHS declares that Russia is behind hacking and leaking.

DEC

GHANA

Twitter account of Ghana's electoral commission is hacked and fake results published.

2017

JAN

US

US Intelligence services release joint statement claiming Russian interference in elections

APR–MAY

FRANCE

Bots highly active in French presidential elections, including to promote #MacronLeaks – partly-falsified cache of Macron campaign communications.

Example: Hacking the Democratic National Party (United States, 2016)

The DNC leak consisted of hacked data from seven key members of the DNC: to date nearly 20,000 emails with over 8,000 attachments have been leaked, all written between January 2015 and May 2016 (Peterson 2016). The hacked emails were first released via dcleaks.com, and later by WikiLeaks. Responsibility was initially claimed by the persona Guccifer 2.0 (Franceschi-Bicchierai 2016). The identity of Guccifer 2.0 is widely disputed, and most security analysts and US intelligence agencies link the leaks to Russian intelligence services (Lipton and Sanger 2016; Office of Director of National Intelligence 2017).

MAY

US

Robert Moeller begins investigation into cooperation between Russian government and Trump campaign.

JUN

UK

Parliament email system compromised.

SEP

GERMANY

Right-wing trolls, both German and foreign, promote disinformation and hate in run-up to federal elections.

SEP–OCT

US

Facebook, Google, Twitter and other platforms acknowledge foreign ads and posts during US elections.

OCT

CANADA

Facebook launches "electoral integrity initiative" in Canada.

The organization, timing and promotion of the DNC leaks maximized the reputational harm to the Democratic Party at a key moment in the 2016 campaign (Rid 2016; Savage 2016). The documents were leaked shortly before the DNC's nominating convention in late July, 2016, making them a prominent discussion point at the time of Hillary Clinton's nomination as presidential candidate. The Guccifer 2.0 persona and WikiLeaks drew attention to the leaks and promoted the belief that they revealed corruption in the DNC. The leaks and their negative framing of Clinton and the DNC were amplified by other digital techniques, including being promoted by bots and troll networks.

Example: Macron Leak (France, 2017)

Two days before the final round of the 2017 French presidential elections, a trove of emails and documents that allegedly belonged to the campaign team of candidate Emmanuel Macron was released online (BBC 2017). Links to the stolen data were propagated by a hashtag campaign, #MacronLeaks, which appears to have been heavily promoted by individuals and bots associated with right-wing or pro-Russia operations (DFRLab

2017; Scott 2017). The leaked data was billed as containing nine gigabytes of information, including damaging information about offshore accounts, tax evasion, and other wrongdoing by Macron. In fact, much of the leaked data did not concern the campaign and was "padding" (grugq 2017). The credibility of the leaks was also under-mined by the Macron campaign's claims to have intentionally given false data to hackers (Doman 2017).

DIGITAL MISINFORMATION: FAKE NEWS AND COMPUTATIONAL PROPAGANDA

Political scientists have long been interested and concerned about citizens' knowledge of politics and public issues (Achen and Bartels 2016; Carpini and Keeter 1996). While much attention has been given to the problem of *uninformed* citizens, scholars have also examined the pernicious effects of *misinformed* citizens, who are committed to untrue beliefs (Kuklinski et al. 2000). Concern about the threat to democracy posed by digital media use has increased dramatically, due to the recent rise of "fake news" and active *disinformation* campaigns (Gu, Kropotov, and Yarochkin 2017; Vargo, Guo, and Amazeen 2017). There is now extensive documentation of disinformation campaigns during elections in Brazil, France, Kenya, Ukraine, US, UK, and other countries (Allcott and Gentzkow 2017; Ferrara 2017; Pollock 2017; Woolley and Howard 2017).

This section describes how foreign actors use bots, fake social media accounts, memes, and other techniques to disseminate misinformation and disinformation.

Techniques

Fake news is often defined as misleading information that resembles conventional journalism (Lazer et al. 2017, 4; Vargo, Guo, and Amazeen 2017). Several scholars suggest that *intent* is an important factor in distinguishing the phenomenon that threatens democracy (Allcott and Gentzkow 2017; Gu, Kropotov, and Yarochkin 2017). Knowingly creating and sharing "fake news" is an act of disinformation that is different from the accidental spread of misinformation (Ferrara 2017; Jack 2017; Marwick and Lewis 2017). Intentional misinformation may be propagated for profit rather than political aims (Subramanian 2017).

While fake news may resemble credible journalism, other genres of online misinformation

do not. These include advertisements, videos, and fake endorsements of candidates. Memes, too, can effectively promote misinformation, because of their viral spread but also because they are seen as trivial and not fit for discussion and therefore rarely face authoritative corrections (Lyons 2017a). Some research finds that entirely fabricated content is less influential because it is easier to fact-check and correct than "fictitious-information blends," which are more plausible because they maintain one foot in reality (Rojecki and Meraz 2016).

Fake news, memes, and other genres of misinformation do not necessarily have to be digital. However, the reach and potential influence of misinformation is greatly expanded when "the use of algorithms, automation, and human curation [is used] to purposefully distribute misleading information over social media networks" (Woolley and Howard 2017, 4). Furthermore, the porous border between social media and hyper-partisan media outlets creates an "alternative media ecosystem" that enables online misinformation to be amplified on television, on the radio, or in newspapers (Benkler et al. 2017; Starbird 2017).

Apart from the organic spread of misinformation between users, the primary digital techniques used to disseminate misinformation are known as "bots" and "sock-puppets."

Bots are "algorithmically driven computer programs designed to do specific tasks online" (Woolley and Howard 2016, 4885). McKelvy and Dubois (2017) propose four types of political bots: *dampeners* suppress messages, *amplifiers* make messages appear more popular than they are, *transparency bots share* information relevant to informed citizenship, and *servant bots* are used by government and organizations to answer questions or provide other services. Bessi and Ferrara (2016) find that bots are primarily used on Twitter to rebroadcast content, rather than reply to others, although rebroadcasting might be used to dampen messages or amplify others.

Sockpuppets are "human-operated fake accounts" (Morgan and Shaffer 2017), which enable actors to hide or misrepresent their identites. Sockpuppets can be used to make messages more credible, such as by impersonating a trusted source make it appear that particular people or groups are spreading messages or hold opinions that they do not – such as an apparently Russian-controlled account "United Muslims of America" that attacked US politicians and promoted misinformation about US foreign policy (Collins, Poulsen, and Ackerman 2017). Multiple fake accounts can also be also used to amplify

messages. For instance, sockpuppets were used to share pro-Trump and anti-Semitic messages on social media during the 2016 US election (Morgan and Shaffer 2017).

Bots and sockpuppets can be purchased (Gu, Kropotov, and Yarochkin 2017; Morgan and Shaffer 2017; Thomas et al. 2013), though Russia, China, and other governments may task staff to act as sockpuppets (Aro 2016; Bradshaw and Howard 2017; G. King, Pan, and Roberts 2017).

Not only can messages be massively amplified on social media platforms, the design of these platforms often has the additional effect of exposing readers to sensational headlines with little contextual information, while simultaneously promoting its purported veracity due to the fact that it was shared by friends or other trusted proxies. Whether intentional or not, these features take advantage of human psychology and can leave citizens more likely to believe misinformation (Allcott and Gentzkow 2017; Gu, Kropotov, and Yarochkin 2017; Messing and Westwood 2014).

Example: Fake News in the 2016 US Election

The recent US election generated extraordinary amounts of fake news (Bell and Owen 2017, 68–71; Vargo, Guo, and Amazeen 2017). In the last months of the election, the top 20 fake news pieces had greater engagement on Facebook than the top 20 stories from major news outlets (Silverman 2016). Fake news sites were operated by domestic and foreign actors, including transnational right-wing networks and Macedonian teenagers (Subramanian 2017). In late 2017, it was revealed that Russian actors purchased political ads and used fake identities to post fake stories on Facebook and other social media platforms (Collins, Poulsen, and Ackerman 2017; Isaac and Wakabayashi 2017). False stories on Facebook – such as the Pope endorsing Trump – were more likely to benefit Trump and the Republican Party rather than Clinton and the Democratic Party (Allcott and Gentzkow 2017; Benkler et al. 2017; Silverman 2016).

Example: Bots and the 2017 French Election

There is considerable evidence that bots were used to influence the recent presidential election in France (Desigaud et al. 2017; Howard et al. 2017). Hundreds of social media accounts – including many that were active during the 2016 US election – promoted false and defamatory information, primarily against candidate Emmanuel Macron. These accounts were particularly active in the final days of the election, when they promoted the

possible leak of Macron campaign documents (DFRLab 2017; Doman 2017; Scott 2017).

However, the effect of this misinformation seems to have been limited as most engagement with these bots came from foreigners and French citizens already on the extreme right (DFRLab 2017; Ferrara 2017). Furthermore, the dissemination of leaked information was limited by its timing, by decisions of journalism outlets not to give the leaks extensive coverage (for legal and professional reasons), and by the electoral commission's prohibition on publishing hacked documents during the legal blackout period immediately preceding the election (Donadio 2017; Willsher 2017).

MANIPULATING PREFERENCES VIA BIG DATA AND MICRO-TARGETING

Digital technologies enable mass data accumulation and the increasingly specific targeting of groups and individuals with messages meant to persuade or mislead them. While targeted messaging and data accumulation have long been a part of democratic campaigns, their use has expanded due to an exponential growth in the accumulation and computational processing of data, and through algorithm-enabled targeting and testing of messages. As a result, the potential for micro-targeted *manipulation* has greatly increased.

Compared to the pre-digital era, foreign actors have significantly greater and easier access to data than in the past, making extraterritorial electioneering easier and more effective (Cadwalladr 2017a; Teachout 2009). Targeted influence operations, which in the past had to be carried out near to targets, can now be done from a great distance – even from another state. Through surveillance and micro-targeted messaging, foreign actors can now manipulate people in ways that undermine or shape their political participation, or that may turn them against fellow citizens.

Techniques

Micro-targeted manipulation requires that actors have extensive data about potential targets, that they can identify targets (often using algorithms) and disseminate messages to them, and that they can design messages that are likely to influence their targets opinions or actions.

Digital technologies make it possible to collect mass amounts of information about

populations, or about specific groups and individuals. Data can be acquired in several different ways. Social media platforms, search engines, and websites gather huge amounts of data about users, and track their actions and movements online, as part of their advertising model (Albright 2017; Christl 2017). This data can be sold to foreign actors legally or in black markets, or acquired by foreign actors by hacking databases (Lewis and McKone 2016; Vijayan 2015).

People's data is also acquired by governments, including information about government employees (Gilman, Goldhammer, and Weber 2017) and about citizens in general (Perlroth, Wines, and Rosenberg 2017). As Hersh (2015) shows, political parties in the US have shaped public policies to acquire data about citizens that they can use for electoral strategies. In addition, law enforcement and intelligence agencies engage in mass and targeted collection of the communications of citizens and non-citizens (Greenwald 2014; Privacy International 2016). Such data may be shared with or hacked by foreign actors (Gilman, Goldhammer, and Weber 2017; Nakashima 2017).

Foreign actors thus have significant *legitimate* access to data relevant to people's political participation and mobilization, such as by following their social media feeds or purchasing information from data brokers. They also have *illegitimate* means to get this data, such as through hacking or surveillance operations.

Algorithms are used to rapidly sift through these massive amounts of data to identify relevant sub-populations that may be targeted. Algorithms can identify people based on demographics, geography, psychographics, behaviour, and combinations of each of these categories. Pernicious targeting is possible. For instance, *ProPublica* revealed that Facebook allowed advertisers to target algorithmically-identified "Jew haters" (Angwin, Varner, and Tobin 2017), and another study suggested that algorithms could identify homosexuality – raising concerns about state tracking and abuse (Kosinski and Wang forthcoming).

A further concern about micro-targeted messaging is that it may evade public scrutiny, since the algorithms used tend to be complex and proprietary, and since micro-targeted messages are not typically visible to general publics. Perhaps most notable is Facebook's former practice of allowing 'dark posts', which were only visible to targeted audiences (Baldwin-Philippi 2017; Lapowsky 2017). In the 2016 US election, the Trump campaign's dark posts "included videos aimed at African-Americans in which Hillary Clinton refers

to black men as predators" (Grasseger and Krogerus 2017). The lack of transparency of algorithms and message content makes it difficult for individuals or institutions to scrutinize, check, or refute micro-targeted messaging (Yeung 2017).

Micro-targeted messaging may sometimes provide people with better and more relevant information, including on political issues. However, there is widespread concern that micro-targeting can facilitate *manipulation*. Manipulation occurs when an actor uses deceptive means to induce changes in people's thoughts or behaviors, in ways that people would not have endorsed had they been aware of the deception (Goodin 1980).

Manipulation may be easier with micro-targeting for several reasons. First, messages can be customized to fit specific audiences, and designed to exploit specific cognitive dispositions and information deficits. For instance, highly-charged affective messages can be targeted to low-information voters (Gorton 2016). In effect, "hacking the brain" (Fonseca 2010; Kahan 2013).

Second, micro-targeting allows actors to target specific groups (or individuals), and to precisely control the timing, information, and sites of contact, so that they leverage psychological predispositions or vulnerabilities for maximum effect.

Third, micro-targeted messages are usually only seen by targeted audiences, limiting possibilities for critique or counterargument. This technique can thus reduce the "publicity" of political messaging.

Finally, micro-targeting could be used to identify and mobilize potentially dangerous individuals or groups within a political community, targeted at specific groups or individuals to incite backlash or even violence. Groups or individuals could be targeted with particular messaging (e.g. misinformation, fake scandals, etc.) designed to incite them, by playing on confirmation or in-group biases, bandwagon effects, motivated reasoning, or psychological state (e.g. depression or delusion).

Example: Mobilizing conflict in the 2016 US election

Micro-targeting played a role in mobilizing pro-Trump support and rallies during the 2016 US campaign. Russian actors are believed to have purchased at least 3,000 micro-targeted Facebook ads to influence Americans (Isaac and Shane 2017; Stamos 2017). Facebook estimated that approximately 10 million people saw these ads, and that the

ads and other posts by Russia-affiliated actors reached 126 million people (Isaac and Wakabayashi 2017). Russian propagandists are also suspected to have organized rallies. In Florida, pro-Trump rallies were facilitated with data from Facebook (via a page called "Being Patriotic") and Twitter (through the account @march_for_Trump) (Collins et al. 2017). The Facebook page (now closed) was run by the Russia-based Internet Research Agency. Russian actors are also believed to have organized competing demonstrations in Houston, supporting and opposing Muslims in the US (Lister and Sebastian 2017).

Example: Psychographic profiling in the US election and Brexit referendum

The US-based company Cambridge Analytica and associated organizations have come under scrutiny for assistance in micro-targeting campaigns in both the US election and the UK's Brexit referendum (Cadwalladr 2017b). Cambridge Analytica claimed to be able to micro-target US voters with messages based on their personalities and emotional states, using "psychographic" evaluations drawing on thousands of data points about every American (Illing 2017). While Cambridge Analytica played a key role in the Trump campaign, there are significant doubts about whether this psychological manipulation occurred or was effective (Illing 2017; Tworek 2017a). In the case of the Brexit referendum, a Cambridge Analytica contractor assisted several pro-Leave groups to micro-target advertising, and may have violated campaign laws (Cadwalladr 2017b).

INTERNET TROLLING

Uncivil, threatening and disruptive behaviours online are frequently referred to as "trolling." While such behaviours are not new to democratic politics, DCTs have introduced new techniques and opportunities. Crucially, DCTs enable a scale shift in the coordination of trolling behavior. Such large-scale trolling activity may have pernicious effects on a society's communication styles and political culture.

While some researchers define a troll as any person who intends to "cause disruption and/or trigger or exacerbate conflict for the purposes of their own amusement" (Hardaker 2010), others contend that such a view implicitly adopts trolls' own views of themselves as iconoclastic mischief-makers (Phillips 2015). We instead follow Forestal in defining trolling as:

[A] specific kind of political activity that is marked by a refusal to participate in the kind of productive exchange of ideas that marks democratic politics. Instead of engaging in activity marked by democratic principles of reciprocity, accommodation, and inclusion, trolls actively work to dominate and control the conversations on any given site. (2017, 150)

Research on foreign interference in elections through online trolling is growing. For instance, there is extensive evidence of Russian government funding of troll networks to wage information warfare and influence public opinion during elections (Aro 2016; Greenberg 2017; Spruds et al. 2016).

Techniques

Threat-making and intimidation are key trolling tactics. Common forms of intimidation include death threats, threats of sexual assault, threats of violence to family, or threats of smear campaigns and reputational damage (Bradshaw and Howard 2017; Garofalo 2016; Massanari 2017; O'Carroll and Escorcia 2017; Spruds et al. 2016). Pro-government troll mobs have targeted journalists, political dissidents, and opposition parties with such threats. Threat-making often draws on longstanding antagonisms or vulnerabilities that exist in societies. For example, women are frequently targeted with threats of gendered violence, such as the trolls loyal to Turkey's Justice and Development Party who target women journalists with rape threats (Shearlaw 2016); Russia-backed trolling efforts often seek to inflame ethnic tensions (Collins, Poulsen, and Ackerman 2017; Spruds et al. 2016); and trolls aligned with transnational alt-right groups promote stigmatization of people of different racial, ethnic, gender and religious identities (Nagle 2017; Phillips 2015).

Another common method of intimidation and harassment is *doxxing*. Doxxing "starts with publishing someone's personal information in an environment that implies or encourages intimidation. Typically done online, the information then is used by others in a campaign of harassment, threats and pranks" (Henrichsen 2015). The unwanted publicity of one's personal information is the opposite of the anonymity the doxxers enjoy and preserve for themselves. Trolls are therefore able to control who has access to anonymity and who does not, allowing them to act with relative impunity while making their targets insecure. Many critics link doxxing with an online culture of organized misogyny that seeks to prevent women from participating in online spaces (Mantilla 2015).

A third method of trolling is the creation of trivializing or stigmatizing *memes*. Memes

may be used to increase cultural and political polarization, while seeking to trivialize threatening behaviour. One high-profile example is the association of racist or white nationalist messaging with the image of "Pepe the Frog" (Marwick and Lewis 2017, 36).

Finally, trolling is increasingly integrated with the propaganda efforts of governments and political parties. Bradshaw and Howard document the widespread existence of "government, military or political party teams committed to manipulating public opinion over social media" (2017, 3). These state-sponsored trolls often target journalists, government critics and political dissidents. For example, cyber agents with connections to the Azerbaijani, Mexican, and Russian governments have targeted political opponents and journalists (Duncan 2016; Geybulla 2016; O'Carroll and Escorcia 2017). King et al (2017) have estimated that agents working for the Chinese government post approximately 448 million social media comments every year.

The Russian government has received particular attention for paying "troll armies" to comment on social media platforms to shape public debate (Aro 2016). A report by the NATO StratCom Centre for Excellence details the Russian use of trolls that "communicate a specific ideology and, most importantly, operate under the direction and orders of a particular state or state institution" (Spruds et al. 2016, 10). The strategic aim of this trolling is to undermine public trust in the credibility of an opponent government through systemic information warfare (Ibid, 14).

Not all comments by regime-sponsored agents are abusive. For instance, agents directed by the Saudi Arabian government posted ostensibly neutral content with the apparent aim of distracting people from the original discussion (Freedom House 2013). A similar tactic, and one more consistent with the ethos of troll as provocateur, is posting incendiary material to provoke outrage among other participants, drawing attention toward the troll and away from the substance of the political issue previously being discussed (Bradshaw and Howard 2017).

Examples: Trolling the 2016 US election and 2017 German election

Trolling played a significant role in the 2016 US presidential election. Numerous commentators observed the use of trolling tactics, in particular by Trump and Trump supporters, to organize harassment campaigns against opponents and journalists (Aiken

2016; Spike and Vernon 2017). The voting process itself was disrupted by trolls who targeted prospective Democratic Party voters with misinformation about where and how to vote (Eordogh 2016). Foreign government-sponsored trolls also promoted fake news (Collier 2017; Rainie, Anderson, and Albright 2017).

The connection between politically-motivated trolling and far-right candidates and parties has been observed in European elections. During the 2017 German federal elections, trolls circulated hate-infused memes and misinformation to garner support for right-wing populist party Alternative for Germany (Applebaum 2017; von Hammerstein, Höfner, and Rosenbach 2017). The AfD benefitted from fake and inflammatory misinformation produced by non-Germans, including those from Russia and the US (Hjelmgaard 2017).

WHAT ARE THE IMPACTS OF THESE THREATS?

Foreign actors have been shown to use a range of digital techniques to influence elections. Strong evidence about the effects of this meddling is limited, however. For instance, we have not found a conclusive case in which foreign interference using DCTs changed the outcome of an election from one candidate or party to another.

This section summarizes key findings about how digital techniques – sometimes in conjunction with one another – can impact not just election outcomes, but the key democratic activities of participation, public deliberation, and institutional action.

Participation

Evidence suggests that foreign actors can use digital techniques to undermine citizen political participation in a variety of ways. These techniques range in targets, with some affecting people generally, some focused on supporters of particular parties, and some used to exclude people from participation on the basis of their identity or socio-economic status.

The most basic form of democratic participation, the ability to vote and have one's vote count, is threatened by digital interference. There is evidence that foreign actors have gained access to voting systems and databases, although there is no documented evidence that foreign actors have successfully changed electoral outcomes this way (see more on hacking of voting processes and electoral commissions in the Institutional Action sub-section below). People's ability to vote may also be threatened by misinformation operations that actively spread misinformation about how and where people may vote (Eordogh 2016).

Misinformation can also be used to discourage voters to go to the polls. Existing research on elections suggests that campaign ads very rarely persuade citizens to change who they will vote for (Kalla and Broockman 2017). Ads appear can be more effective at increasing or depressing voter turnout, and at influencing whether people will vote for lesser-known candidates (Holtz-Bacha et al. 2017; Krupnikov 2014). It is not yet

clear whether micro-targeted advertising has more significant effects on voters' choices or turnout.

Democratic participation may also be undermined by actors who use digital techniques to blackmail, threaten, or harass candidates or other individuals who seek to participate in elections and in public debates. Concerns about hacking operations to enable blackmail were raised by MPs in the UK when 90 parliamentary email accounts were compromised in 2017 (Guardian Staff 2017). The persistent threat of attacks on private data may dissuade people running as candidates or advancing certain public positions. Moreover, the exposure of supposedly private data and communication imperils privacy rights and freedoms of conscience, communication and association (Parsons 2015).

Trolls target candidates for public office with threats and harassment, seeking to discourage their participation (Garofalo 2016). As one of many examples, Kim Weaver recently dropped out of an Iowa congressional race, partially because of online death threats (Doyle 2017). Online trolling frequently targets vulnerable groups that already face barriers to full participation, including women, and ethnic, racial, religious or gender minorities (Massanari 2017; Nagle 2017). Indeed, much of what is colloquially categorized as trolling is indistinguishable from criminal threat and hate speech (Citron 2014). Trolling by sockpuppets amplified anti-Semitic and nativist language on social media and partisan news sites during the 2016 US election (Morgan and Shaffer 2017).

Trolls may attempt to poison the waters of online discussion to discourage citizens or groups from participating in discussions about specific political or social issues, particularly during elections. Aro (2016), for example, interviewed many people who stopped making Russia-related comments online out of fear that they would continue to be targeted by trolls.

More generally, those who purchase or create computational propaganda mechanisms can drown out contributions by other voices on social media platforms. For instance, research suggests that a single Russian agency purchased over 3000 Facebook ads that were shared hundreds of millions of times (Timberg 2017). Even a small number of bots can produce a large number of tweets (Starbird 2017), especially if influential human users retweet their content (Chengcheng Shao et al. 2017). Bessi and Ferrara (2016) estimate that bots were responsible for up to 20% of US election tweets. Similarly, half of English-language #Macronleaks tweets originated with only 5% of users (Scott 2017)

and 6% of all French-election tweets included fake news (Desigaud et al. 2017).

Strategic ad buys, the use of bots and trolls, and other strategies, can thus enable messaging by foreign actors to eclipse citizen voices.

Public Deliberation

During the periods of intense public communication before elections, citizens and candidates and civil society groups all put forward their views in a wide range of forums and platforms. Not only does this communication inform whether and how people will vote, it also helps to establish collective understandings about the issues and values at stake.

Foreign actors can use DCTs to push false or misleading information, or can suppress and filter information flows, in ways that *undermine the epistemic quality* of public deliberation. This not only leads to weak understanding of public issues and disagreement on facts, but can also lead to belief in dangerous conspiracy theories (e.g. #pizzagate, voter fraud) (Martin 2017; Marwick and Lewis 2017; Peters 2017). Misinformation can be taken up by powerful individuals as well as voters. Feinberg (2017) reports on a Republican staffer who helped draft an amendment to a bill that took as its basis misinformation found on a pro-Trump subreddit.

There are two often theorized mechanisms for people's uptake of misinformation. The first explanation posits that individuals may be susceptible to 'fake news' because they process it using automatic, rapid, and non-conscious modes of 'fast' thinking rather than the conscious and cognitively taxing modes of 'slow' thinking (Kahneman 2011). On this view, fake news persuades readers who do not think carefully about what they are reading. The second explanation suggests that individuals may engage in motivated reasoning, which aims not at accuracy but at reaching a conclusion that is congruent with one's prior beliefs. Motivated reasoning in this context is often driven by partisan considerations, including political beliefs and partisan self-identification.

Pennycook and Rand (2017b) find the lack of analytic thinking, rather than partisan motivated reasoning, explains susceptibility to believing "fake news" headlines. However, partisan considerations might motivate sharing "fake news" online. Social media platforms are designed to take advantage of these cognitive limitations to encourage "virality", which can lead users to share politically concordant fake headlines on social

media, even if they are unsure of their accuracy (Pennycook and Rand 2017b, 36). The increased use of *social* media as a source of information also offers an opportunity for people to make their own news consumption a marker of group membership, sharing information to protect "one's identity or standing in an affinity group that shares fundamental values" (Kahan 2013, 408). As partisans have become increasingly hostile to opposing parties (Iyengar and Westwood 2015), sharing propaganda journalism may also be used to provoke or harass those who do not share partisan affiliation, especially given the willingness of hyper-partisan media outlets to publish material that targets specific groups (Bernstein 2017).

Hyper-partisan media outlets use click-bait headlines, memes, and other rhetorical devices to encourage amplification of misinformation by both human and bot users of various social networks (Faris et al. 2017; Woolley and Guilbeault 2017). For instance, memes made up Breitbart's most-shared posts during the 2016 election and were potent vectors for misinformation (Lyons 2017a; Marwick and Lewis 2017). Amplification gives the appearance of widespread belief in false information and encourages the mainstream media to report on it (Chadwick, O'Loughlin, and Vaccari 2017; Manjoo 2017). Reporting on disinformation often requires repeating it, which can increase its salience (B. Weeks and Southwell 2010) or influence readers even if accompanied by a correction (Vargo, Guo, and Amazeen 2017).

These misinformation strategies may seek to convince people to adopt particular opinions or take particular actions. However, they may also aim to systematically exhaust citizens' search for truth or their trust in political institutions by using a "firehose of falsehood" propaganda model (Paul and Matthews 2016), which can lead people to see "question the integrity of all media as equally unreliable" (Citizen Lab 2017).

In addition to promoting falsehood, digital techniques are used to *shape the agenda* of public deliberation. For example, bots are used to amplify favourable messages and dampen criticism of the Russian government without resorting to censorship (Sanovich 2017). Bots were used in the US election campaign to "manufacture consensus" by amplifying messages and producing the appearance of online popularity and offline political support (Bessi and Ferrara 2016; Woolley and Guilbeault 2017). Similarly, sockpuppets have been used to stop political argumentation in China, where government employees post millions of benign messages on social media to drown out public awareness of direct action against the government (G. King, Pan, and Roberts 2017).

Hacking operations can contribute to these information operations that seek to shape the agenda of public deliberations. High-profile leaks of hacked documents can also be used to distract publics from other issues or candidates. For example, the first leak of John Podesta's emails came an hour after the infamous Trump's infamous *Access Hollywood* video was released, and the Podesta leaks were dribbled out in the weeks before the election to maintain attention (Lubben 2017).

In their general overview of agenda-setting in the 2016 US presidential election, Faris et al. (2017) examine both mainstream and social media coverage and contend that asymmetric partisan polarization among media outlets allowed the Trump campaign to set the agenda around its proposed policies while the Clinton campaign became synonymous with scandal.

In contrast, the #MacronLeaks release appears to have failed to change the agenda during the 2017 French presidential election. Possible reasons include the leaks' timing (just before the election, during a media blackout period), the different media environment (with gatekeeper media outlets that were unwilling to publish quick takes on the leaked data), a different political culture in France (less partisan on party lines), and the existence of a widespread public narrative about the likelihood of Russia-backed leaks and misinformation campaigns (Dickey 2017). Furthermore, the French electoral commission, in an emergency session, warned media and internet users that they could face criminal prosecution if they published the hacked documents (Donadio 2017; Willsher 2017).

Misinformation and propaganda can also be mobilized to *promote division and distrust*. Misinformation can be created, disseminated and targeted in ways that amplify existing divides, such as partisan conflict, in order to drive wedges between allies and undermine shared norms of democratic debate (Canadian Security Intelligence Service 2017; E. King 2016). For example, some Russian-purchased Facebook ads focused on polarizing issues – such as gun control and immigration – in an apparent attempt to amplify social discord (Isaac and Shane 2017). Other Russian-orchestrated social media messages promoted violence among social factions in the US, including along racial and religious lines (Devine 2017; Lister and Sebastian 2017).

Institutional Actions and Electoral Regulation

Foreign actors can use DCTs to block or hamper institutional actions necessary for elections, and to violate electoral regulations.

Electoral commissions and other state bodies that oversee voting processes face cyber attacks. For example, a hacking attack on central servers of the Ukrainian voting authority in 2014 deleted important files just before the election, and its public reporting systems were compromised and only fixed an hour before false election results were announced (Clayton 2014). In 2016. the website of Ghana's Central Election Commission was hacked and false results were tweeted from the Commission's account while votes were still being counted (Communications Security Establishment 2017, 17). Kenya's supreme court annulled the country's August 2017 election, in part because some evidence suggested the voting system had been hacked (Dahir and Kuo 2017). In the US, there is evidence of theft and possible manipulation of voter lists in dozens of states, as well as evidence that hackers affiliated with Russia's military intelligence attempted to access the computers of 122 election officials prior to the election (Calabresi 2017; Kopan 2017). Hackers were able to access – and in one case possibly change – the electronic poll books used at polling offices to confirm eligible voters (Perlroth, Wines, and Rosenberg 2017). There have also been proof of concept tests showing that voting processes and databases can be hacked by outside actors, leading to calls for reform in the United States and beyond (National Election Defense Coalition 2017; Norden and Vandewalker 2017). These hacking attempts can lead voters to question the integrity of the electoral system and the value of their participation.

The hack and release of data can also present serious obstacles to political parties and civil society organizations, which must address security risks to personnel; economic exposures; and derailed communication strategies. For organizations, the costs of responding to data breaches and leaks can range from hundreds of thousands to hundreds of millions of dollars (Crootof 2018, 30). Even if hacked data is not publicly leaked, it can be used or shared to give some actors an unfair or strategic advantage over electoral competitors. In the 2012 presidential election in Mexico, "a team of hackers ... stole campaign strategies ... and installed spyware in opposition offices, all to help Peña Nieto, a right-of-center candidate, eke out a victory" (Robertson, Riley, and Willis 2016, 61).

Trolling operations can also be directed at public officials involved in voting processes,

and troll networks have been encouraged to develop hashtags and memes to target public officials. Civil society watchdogs and journalists have all been targeted by troll networks during elections, thereby undermining their ability to hold public institutions to account.

Foreign actors may also violate the letter or spirit of electoral and criminal regulations using DCTs. It is clear that Russian actors violated limitations on campaign spending in the US elections. In the UK's Brexit referendum, a Canada-based company with ties to US-based Cambridge Analytica may have violated campaign laws in the UK's Brexit referendum, by counting as undeclared and impermissible foreign donations (Cadwalladr 2017a). More generally, it is extremely easy to hide the location or identity of authors of websites, social media posts or bots, making election regulations on campaign spending and media broadcasts extremely difficult. The German, US, Canadian, and other governments have announced their intention to update laws and enforcement mechanisms to address these gaps in regulation (Kinstler 2017; Klobuchar 2017; Standing Senate Committee on Legal and Constitutional Affairs 2017).

WHAT THREAT ACTORS EXIST, WITH WHAT INTENTIONS AND CAPABILITIES?

Many types of actors, with different capabilities and intentions, use digital techniques to influence elections or undermine democracy.

Technical abilities and resources are necessary, but many techniques described in this report do not require significant technical sophistication. For instance, it is relatively easy to create or purchase bots, or to set up social media accounts for trolling. By contrast, mass surveillance and some forms of cyber intrusion and extraction require significant technical resources.

In addition to technical capabilities, threat actors draw on "social capabilities," such as knowledge of their targets, techniques of social engineering, or knowledge of strategies to influence particular media or political systems (Citizen Lab 2014; Communications Security Establishment 2017). For instance, when examining the capacities of actors to mount digital threats against Canadian elections, Canada's Communications Security Establishment (CSE) suggests that three areas need to be assessed to evaluate the capability of threat actors: "Technical sophistication of the cyber capabilities," "Knowledge of Canada's democratic process and how it can be manipulated," and "Ability to orchestrate activities and people."

States regularly use DCTs to advance their geopolitical aims (Buchanan 2017), and have been building up both cyber-offensive capabilities and social media "troops" (Bradshaw and Howard 2017). Cyber-criminal organizations sell software or labour (e.g. troll networks) that can be used to interfere in elections (Gu, Kropotov, and Yarochkin 2017). Non-state actors can mobilize many digital techniques, whether as formal networks such as terrorist groups like ISIS (Lee 2016), or informal networks such as right-wing movements that promoted #MacronLeaks in the 2017 French presidential election (Scott 2017). Indeed, alt-right or far right networks have been under the spotlight both for their innovations in digital techniques, and for their white supremacist, anti-feminist, anti-Semitic, neo-Nazi, Islamophobic, queerphobic, authoritarian and ultranationalist elements (Hannan 2017; Nagle 2017).

Canada's CSE proposes the following typology of actors and motivations (2017, 12):

- ***Nation-states*** are motivated by economic, ideological, and/or geopolitical interests.
- ***Hacktivists*** are motivated by ideological issues.
- ***Cybercriminals*** are motivated by financial profit.
- ***Terrorist groups*** are motivated by violent extremist ideologies.
- ***Political actors*** are motivated by winning political power domestically.
- ***Thrill-seekers*** are individuals seeking reputational or personal satisfaction from successful hacking.

These categories are not mutually exclusive. For instance, surveillance technology companies or micro-targeting companies like Cambridge Analytica profit from their services and promote an ideology (Cadwalladr 2017b; Privacy International 2016). Furthermore, social media companies can be considered foreign actors with respect to most countries, they pursue their own corporate and (often implicit) ideological interests (Fuchs 2017; Gillespie 2010), and they may be said to interfere in elections to the extent that they shape people's contributions to public debate and create vulnerabilities to information operations.

Clearly, states are not the only threat actors, and some have argued that cyber technologies may significantly reduce the monopolization of power by states in the international system (Owen 2015). However, state actors are distinguished from non-state actors by their ability to combine sophisticated cyber capabilities (either possessed by their own personnel or purchased), extensive intelligence of targets, and long-lasting, multi-dimensional campaigns of coordinated action on multiple fronts (such as bot-driven propaganda, state broadcast propaganda and troll-networks that can operate in multiple languages) (Aro 2016; Bradshaw and Howard 2017). Moreover, states can coordinate their digital activities with large-scale "non-digital" activities, such as diplomatic campaigns, crackdowns on activists, or military actions. As a result, electoral interference using DCTs may have more extensive and serious effects when coordinated by states.

Most research on state interference in elections using DCTs has focused on Russia. The Russian state promotes misinformation and sponsors hacking attacks on organizations and individuals, using government employees, government contractors, and criminal organizations (Aro 2016; Citizen Lab 2017; Zhdanova and Orlova 2017). Russia is considered to be likely to pursue digital interference in future elections (Communications Security Establishment 2017; Stelzenmüller 2017).

Other states may engage in foreign digital election interference. Taiwan has faced an influx of pro-reunification propaganda that is spread online but originates in mainland China (Monaco 2017). Hong Kong activists have been subject to hacking attacks, and the malware used in these attacks has also been found on the website of Myanmar's national electoral body (Brooks, Dalek, and Crete-Nishihata 2016). While responsibility for these attacks is unconfirmed, it is clear that there are multiple digital strategies being used to interfere in elections in Asia.

The US, UK, Israel, and other states, also have military, intelligence and diplomacy operations that use social media to influence external groups (Bradshaw and Howard 2017). While it is not clear that the US interferes in elections using the digital techniques described in this paper, it has a history of interference (Levin 2016) and the capabilities to do so.

Finally, it is important to recognize that domestic actors often work as de facto "partners" in these efforts. For instance, in the 2016 US election, different actors hacked and leaked the DNC's and Podesta's private data, and these materials were then propagated by mainstream journalism organizations, fake news sites, Republican politicians, and interested citizens (Collier 2017; Legum 2017; Nyhan and Horiuchi 2017). The 2017 French and German elections also saw coordinated actions between foreign and domestic actors, primarily on the political far right, to push misinformation and social conflict (DFRLab 2017; Hjelmgaard 2017).

WHAT ARE THE KEY VULNERABILITIES TO DIGITAL THREATS AND WHAT COUNTER-MEASURES CAN BE TAKEN?

Foreign actors exploit systemic and institutional vulnerabilities when using DCTs to interfere in elections. Our synthesis of existing research suggests there are five key vulnerabilities: deficits in citizens' digital literacy and data protection, polarized political cultures and media systems; problematic social media design and policies; inadequate electoral and criminal regulations; and inadequate international norms and laws on cyber interference. These vulnerabilities affect different political systems in different ways, and comparative research to assess these differences is needed.

This section clarifies these vulnerabilities and identifies counter-measures that have been proposed to address them. To date, there is little robust evidence regarding the effectiveness of these measures.

DEFICITS IN DIGITAL LITERACY AND DATA PROTECTION

People are susceptible to misinformation, manipulation, hacking and trolling in part because of deficits in their use and understanding of DCTs, as well as the insecurity of their private data.

Citizens with less digital literacy are less able to assess trustworthiness or origins of digital messaging and are more prone to manipulation. Even digital natives struggle to determine which news sources are fake and which ones are real (Stanford History Education Group 2016; Stecula 2017). Since coordinated or algorithmic production of content means that the same misleading news stories appear on many different sites, readers can falsely believe they have verified information by checking against multiple sources (Rojecki and Meraz 2016; Sollenberger 2017).

In addition, as Herring et al (2011, 381) note, trolls often "prey on inexperienced Internet users and populations that are vulnerable for other reasons."

Citizens often fail to follow adequate cyber-security practices, as do individuals in political parties, civil society organizations and government agencies. In 2016, the Institute of Information Security Professionals produced a survey in which 80 percent of security professionals claimed that individual behaviours were the most significant challenge to cyber security (IISP 2016). In 2017, Pew noted that many do not trust others to protect their data online but do not themselves follow best security practices (Olmstead and Smith 2017).

Private corporations and government are critical targets given that they collect and keep huge amounts of data. There is widespread concern that neither private nor public actors have adequate measures or adequate incentives to protect people's data (Gilman, Goldhammer, and Weber 2017; Hare 2016). For instance, Roy (2016) argues that Canada does not yet have adequate governance practices to ensure the privacy and security of Canadian citizens' meta-data.

Countermeasures

Digital media literacy and civic education are necessary for citizens to be less vulnerable to online misinformation, propaganda, and manipulation. While digital media literacy is widely endorse, there are disagreements about what it entails and what forms of education are most important (Maksl et al. 2017). There is some evidence of success for models of media literacy that encourage readers to be prepared for exposure to misinformation and to engage in the "conscious processing of information" (Craft, Ashley, and Maksl 2017). However, citizens often lack both the motivation and capacities needed to assess content in fragmented media environments (Lazer et al. 2017). Young people, whose identity and political awareness have developed on social media and in a very polarized era, require particular attention and education (Kahne and Bowyer 2017).

Given contrasting evidence and approaches, a report for the Council of Europe recommends that a task force be established to identify best practices in education that addresses:

(i) traditional news literacy skills; (ii) forensic social media verification skills; (iii) information about the power of algorithms to shape what is presented to us; (iv) the possibilities but also the ethical implications offered by artificial intelligence; (v) techniques for developing emotional scepticism to override our brain's tendency to be less

critical of content that provokes an emotional response; and (vi) statistical numeracy (Wardle and Derakhshan 2017, 70).

One promising recent development was a coordinated project of journalism newsrooms, universities, nonprofits and tech companies to challenge rumors and fabrications in the 2017 French election, which appears to have gained widespread support and increased media literacy by journalists and members of the public (Smyrnaios, Chauvet, and Marty 2017).

There are ongoing attempts to educate citizens, journalists, civil society members, government staff and politicians on issues of cyber-security and data protection, but evidence on what works is limited. While there are extensive sets of tools and recommendations, it can be challenging to provide people with up-to-date recommendations at an appropriate level of technical sophistication. Some of the best privacy and data protection resources are created by civil society groups, such as Access Now and the Electronic Frontier Foundation, or by the University of Toronto's Citizen Lab (Citizen Lab n.d.).

Many technologists and policy experts argue that putting the onus on individuals to protect their own data is misguided, and that technology companies, internet service providers, and governments should do more to make online activities more secure, including by holding to account organizations responsible for security lapses (Tenove, Delgado, and Woodside 2016).

It's clear that members of groups – such as politicians, electoral officials, media organizations, diaspora of repressive states, and members of stigmatized minorities – have different risks of hacking and trolling, and different encounters with misinformation, and thus require different interventions to enhance their digital literacy and cyber self-protection.

POLARIZATION AND HYPER-PARTISANSHIP IN POLITICAL CULTURES AND MEDIA SYSTEMS

High levels of polarization can generate widespread distrust of political institutions, the media, and one's fellow citizens in ways that lay the groundwork for manipulation by foreign actors (Jarvis 2017; Neudert 2017; Vargo, Guo, and Amazeen 2017). Polarization increases ideological commitment to a party and, as a result, may increase

motivated reasoning around misinformation (Druckman, Peterson, and Slothuus 2013). Partisanship, particularly in the US, is increasingly important to people's identities, leading to the politicization of spaces that are not inherently political, including social media feeds (Iyengar and Westwood 2015).

Polarization may be exacerbated by the existence of homophilous information communities or "filter bubbles", which develop in fragmented and polarized media systems and through the algorithmic curation of information (Lazer et al. 2017; Pariser 2011). These filter bubbles can facilitate misinformation cascades, where incorrect information spreads without readers being exposed to any disconfirming evidence (Carlson 2017; Del Vicario et al. 2016), though some research challenges the belief that social media embed citizens in "filter bubbles" (Margetts 2017; Nelson and Webster 2017).

Research on partisan media suggests that hyper-partisan sources tend to be make those who are already partisan even more partisan, but have relatively little effect on those who would not otherwise seek out partisan information (Levendusky 2013). However, social media rumours and hyper-partisan media can reach broader publics if they influence elite opinion-makers or drive the agenda of mainstream media, a phenomenon often seen in the US but not limited to it (Starbird 2017; Vargo, Guo, and Amazeen 2017; Zhdanova and Orlova 2017). Thus, even if only a small proportion of citizens is exposed to hyper-partisan media and messaging, a much broader segment of society is likely to be exposed to the most potent instances of misinformation.

Foreign actors take advantage of information systems with weakened "gatekeeper" institutions, including professional news media, and with high degrees of distrust of political and media institutions. Comparative national research shows that there are significant differences in degrees of polarization and distrust, and that distrust of news media is much higher in states with high degrees of political polarization (Hanitzsch, Dalen, and Steindl 2018).

Counter-measures

Countermeasures will need to promote civility and democratic ethics among key actors, such as political parties, and identify cross-partisan methods of correcting misinformation. Benkler et al. (2017) conclude their study on the US alternative media ecosystem by suggesting that "Rebuilding a basis on which Americans can form a shared belief is

... the most important task confronting the press going forward." The idea of making political parties more deliberative so that they agree on common issues, rather than just pursuing partisan interests, has been raised by several commentators as a way of responding to polarization (Invernizzi-Accetti and Wolkenstein 2017).

Joint action on political polarization may be very difficult. In the US, polarization is asymmetric, with conservatives moving further to the right than liberals have moved to the left (Hacker and Pierson 2015). Republican voters are more likely to consume fake news (Guess, Nyhan, and Reifler 2018), and much more skeptical of the practice than Democrats (Nyhan and Reifler 2016). Conservatives in Canada are also more distrustful of journalism outlets (Anderson and Coletto 2017).

Existing research suggests that corrections may be most effective if they come from within one's own party (Berinsky 2017), from within one's own social network (Bode and Vraga 2017), or if they are on relatively non-contentious issues (Lyons 2017b). Efforts might be productively oriented toward encouraging these types of corrections with the hope of rebuilding agreement on basic facts across partisan lines. Lazer et al. (2017) suggest that including more conservatives in discussions about misinformation is necessary to make progress on this issue.

Despite many proposals for reducing polarization – improving journalism exposure of extreme partisanship, strengthening political parties, introducing non-partisan primary elections, eliminating gerrymandering, or making voting compulsory (Bawn et al. 2012; Berman 2016; Drutman 2017), it's not clear how to bring about these changes.

SOCIAL MEDIA DESIGN AND POLICIES

As Persily notes, social media platforms "are the new intermediary institutions for our present politics" (2017, 74). The intersection between social media platforms and political participation is critical, but this intersection is only a fraction of what social media do. To a significant extent, the business models, design and policies of social media make them poorly-equipped for handling the demands of democratic politics.

The business models of social media companies like Facebook and Twitter depend on the circulation and sharing of attention-garnering content, rather than accurate or high-quality content (Bell and Owen 2017). Particularly in the case of fake news, there

are economic incentives for foreign and domestic actors to undermine democracy during elections. Unlike foreign adversaries who seek to destabilize democratic governments, these participants may not be malicious, such as the Macedonian teenagers who earned thousands of dollars by creating fake political news and news sites during the US 2016 campaign (Subramanian 2017).

There is also an underground economy dedicated to providing fake accounts and bots for a price, with these accounts responsible for an estimated 50% of spam on Twitter (Thomas et al. 2013). Furthermore, platforms like Twitter are attractive to advertisers because of the size of their user base and have little incentive to cull bots and reveal the true number of human users. It may be the case that Twitter is unable to identify and close many bot accounts, which would also suggest that Twitter's ability to target ads is overstated (Fitzgerald and Shaffer 2017). In either case, economic incentives might actually push Twitter to address its bot problem in the future as brands become more concerned about advertising to fake audiences (Sloane 2017).

Facebook, Google, and other social media platforms have also been designed to accumulate data on users and facilitate micro-targeted advertising. This data-informed targeting is very attractive to advertisers, leading Facebook and Google to dominate the online advertising industry (Bell and Owen 2017). However, micro-targeting may also be exploited, as made clear when Facebook enables advertising to anti-Semites (Angwin, Varner, and Tobin 2017), and when Russian actors can target ads to leverage social tensions or promote fake news (Collins et al. 2017; Isaac and Shane 2017).

Social media platforms are vulnerable to trolling because they are designed to maximize engagement and sell ads, rather than provide structured deliberative forums, uphold norms of democratic communication, or perform information vetting functions As the University of Maryland's Frank Pasquale argues, "Very often, hate, anxiety and anger drive participation with the platform. Whatever behavior increases ad revenue will not only be permitted, but encouraged, excepting of course some egregious cases" (Rainie, Anderson, and Albright 2017). Trolls can thus gain disproportionate influence in setting the agenda of public discussion by framing issues in controversial ways that may go viral but contribute little to productive democratic dialogue.

While all social media platforms have policies to discourage hate speech and online threats, these policies and their implementation remain inadequate. Former Reddit

CEO Ellen Pao noted that attempts to crack down on harassment generated backlash and caused her and her colleagues to receive "harassing messages, attempts to post my private information online and death threats" (Pao 2015). The scale of the problem has also necessitated increased reliance on algorithms, although the limits of technology to grapple with complex questions of censorship has highlighted the continued need for human content moderation (Angwin 2017). However, a recent ProPublica investigation of Facebook led to the platform admitting that its content reviewers had made the wrong decisions in 22 of 49 examined posts (Tobin, Varner, and Angwin 2017), suggesting that human error remains a notable limitation. Lastly, the actual work of enforcing these policies, such as commercial content moderation, is undesirable and poorly compensated (Roberts 2017).

Counter-measures

Social media platforms have experimented with a variety of policies and tools for combatting misinformation and hate speech, but further changes ae needed for these platforms to be inclusive spaces for democratic deliberation.

Various technical solutions have been proposed for addressing misinformation: fact-checking bots, algorithms that flag unreliable sources, promoting comments that contain the word "fake" to the top of news feeds, and browser extensions that block misinformation (Monaco 2017; C. Shao et al. 2016; Wakefield 2017; Zhdanova and Orlova 2017). However, the efficacy of fact-checking is questionable (Berinsky 2017; B. E. Weeks and Garrett 2014; Wood and Porter 2016). A recent experiment suggests that Facebook's policy of flagging articles that have been disputed by third-party fact-checkers does little to encourage resistance to misinformation among readers, since articles that have not been marked as disputed might even be seen as more credible due to an "implied truth effect" (Pennycook and Rand 2017a). Facebook has recently stopped marking articles as 'disputed' and instead has begun to show fact-checks in the "Related Articles" feature, which suggests articles on similar topics when a link is posted, and which may be more effective at preventing the spread of misinformation (Bode and Vraga 2015; Ong 2017). Jarvis (2017) suggests that attempting to combat every piece of misinformation is in fact the goal of misinformation campaigns, and that one of the key roles the mainstream media can play is to be more cautious about how attempts to debunk misinformation can amplify it and increase its potency.

Google and Facebook banned misleading websites from their advertising networks in order to target the economic motivation for producing fake news (Wingfield, Isaac, and Benner 2016). Twitter recently did the same to advertising for Russian state-sponsored media outlets (Twitter 2017).

Implementing naming policies has become one of the more popular proposals for mitigating trolling while compelling users to participate productively. Naming policies require that users share content under their real names, thus tethering a user's reputation to their online behaviour (Forestal 2017). A growing body of research, however, contradicts the belief that real name policies will mitigate online abuse, and finds they can sometimes encourage discrimination based on factors such as race and gender (Matias 2017).

Research on the deliberative capacities of online platforms has begun to identify key design features. Platform designers should pay careful attention to the temporal nature of posts (Friess and Eilders 2015, 325-326), questions of anonymity (Fredheim, Moore, and Naughton 2015; Matias 2017), moderation (Wright and Street 2007), and the architecture of interpersonal interaction, such as how comment threads are structured (Forestal 2017). More attention from academic researchers, including democratic theorists, should be directed toward questions of platform design and use. As Forestal observes, despite the widespread recognition among democratic theorists that democratic politics require norms of reciprocity, accommodation, mutual recognition and trust, there has been extremely little attention to whether and how such norms may be advanced in of digital spaces (2017, 151).

Social media platforms need to change their design and policies to address the ways in which they create vulnerabilities for democracy. New forms of government regulation may be necessary to incentivize platforms to make these changes. In doing so, it need to be recognized that different platforms have different uses and user bases (Kreiss, Lawrence, and McGregor 2017).

WEAK REGULATORY AND ENFORCEMENT CAPACITIES OF STATES

The regulation of campaigns and elections must be re-formulated in a digital era. Governments need to develop the principles and policy levers to address techniques that violate the letter or spirit of existing regulations, and to address new ways in which

foreign actors use DCTs to warp participation and public deliberation and to attack democratic institutions.

The use of social media for political advertising, campaign financing, and other related activity has drawn increased scrutiny as potential and actual violations of existing election laws have received increased attention. Perhaps the most notable apparent violation was the admission by Facebook that Russian trolls spent over $100,000 on election advertisements in the 2017 presidential election. The US Federal Election Commission (FEC) last introduced new regulations for internet advertising in 2006, when social media was still in its infancy. Glaser (2017) reports that the result has been a lack of clarity in the US about the legal requirements for online political advertisements. In 2010, Google claimed that the advertisements were too small to require transparency about who bought them, although the FEC insisted that the advertisements should link to a page that disclosed the buyer. Facebook challenged the need to link to a disclaimer and a tie vote at the FEC led them to proceed without these transparency measures (Goodman and Wajert 2017). In the wake of the 2017 presidential election, the FEC has clarified that advertisements on social media must include a disclaimer about who paid for them (Glaser 2017).

Other countries are grappling with the same issue. The U.K's Electoral Commission has noted that advertising on social media is subject to existing law, but that they do not track this spending and do not know if advertisements were purchased through third parties (Tambini et al. 2017). Elections Canada, notably, has issue a detailed Interpretation Note that concludes that any message that has a "placement cost" and otherwise meets the definition of "election advertising" in the *Canada Elections Act*, is subject to all relevant regulations (Elections Canada n.d.).

Advertisements are only one of several ways that social media can be used to violate the spirit, if not the letter, of relevant laws. For instance, foreign actors can use bots, paid staff or troll networks to promote information without paying social media companies for advertising (Goodman and Wajert 2017). Indeed, "organic posts" by the Russia-based Internet Research Agency appear to have spread content to more Americans than via paid ads (Isaac and Wakabayashi 2017).

Improved regulations of third-party activities, including via online messaging or non-monetary contributions to campaigns, are also needed. The Commissioner of Canada Elections

has warned about the potential for unregulated third-party activities to influence elections by using social media or other online tools, particularly in ways that are not covered by existing advertising regulations (Standing Senate Committee on Legal and Constitutional Affairs 2017). The UK's Electoral Commission has started an investigation into possibly illegitimate foreign campaign donations, through the involvement of Canada-based AggregateIQ, a firm apparently linked to Cambridge Analytica (Elgot and Grierson 2017).

With respect to the spread of misinformation and trolling campaigns, social media companies have economic incentives to minimize their responsibility for user-created content and to avoid legal regulation. To push back against these impositions, companies including Facebook and Twitter often describe themselves as "platforms," rather than media companies, and as defenders of free speech (Gillespie 2010). There is a lack of clarity about whether and how states can regulate speech on social media platforms, particularly platforms that are based in foreign states. While some governments, such as the Czech government, have noted that they plan to issue factual information to try and correct misinformation that threatens "internal security", other states worry about government overreach (Wardle and Derakhshan 2017, 71–72). Indeed, there are concerns that overly "restrictive regulation of internet platforms in open societies sets a dangerous precedent and can encourage authoritarian regimes to continue and/or expand censorship" (West 2017). This problem is complicated by the fact that social media companies have also disrupted journalism outlets that were the pre-existing gatekeepers for information and public deliberation.

Additionally, many states lack the technical and regulatory capacity, or lack the willingness, to identify and prosecute actors who violate domestic and international cybercrime laws. Holding actors to account for cyber attacks is difficult. Obstacles include the problems of attribution and distance—the fact that digital attacks can be obfuscated, and that they may often be launched from anywhere. There are also significant problems of legal jurisdiction and operational coordination, making it difficult to pursue criminal prosecutions or other legal actions against attackers (Citron 2014; Crootof 2018; N. Tsagourias 2016). In Canada, there are several legal avenues to address foreign influence operations, particularly those that are clandestine and that threaten national interests, or that violate regulations on lobbying and campaign spending—but these are hard to enforce, and may be particularly weak at provincial and municipal levels (Carvin and Forcese 2017)

Counter-measures

Governments and civil society are developing a variety of possible regulations to deter the misuse of social media and other DCTs, and to encourage technology companies to implement changes.

In the US, several senators proposed the "Honest Ads Act" to clarify what counts as online political advertising, to maintain public records of political ads that run on social media, and to improve safeguards against political ad purchases by foreign actors (Klobuchar 2017). While many agree the act would improve matters, analysts are concerned that the definitions of prohibited materials are unclear or too narrow, that the social media self-reporting mechanisms are insufficiently robust, and that foreign actors could still make use of dark money groups to purchase advertising online (Goodman and Wajert 2017; Norden, Vandewalker, and Charlton 2017). The Electronic Privacy Information Center further argues that advertisers should not only disclose who bought ads, but also publicize what criteria they used to target those ads to users (Sullivan 2017).

In Canada, too, there is a push to update electoral laws to address the use of DCTs by foreign individuals and organizations. The Senate's Standing Committee on Legal and Constitutional Affairs (2017) has called for revisions of the Canada Elections Act to reduce opportunities for foreign interference via third parties and online advertising or other messages. McKelvey and Dubois (2017) propose that, in addition to amendments in the Elections Act, misuse of political bots could be addressed by modifying and implementing the Canadian Anti-Spam Law, or enforcing criminal laws against harassment, hate speech, and cybercrime.

To address hate speech, threats, libel, and other harmful messaging, some governments have introduced policies to push social media companies to take further actions. Germany passed legislation that requires social media companies to create robust complaint processes, and to remove obviously illegal hate speech within 24 hours or face serious fines (Kinstler 2017; Tworek 2017b). The European Commission proposed a code of conduct to address hate speech without violating freedom of expression, which was signed by Facebook, YouTube, Twitter and Microsoft in 2016 (Hern 2016). The effectiveness of these developments remains unclear, though some users have found that changing location settings to Germany or France on Twitter withholds content that would be illegal under Holocaust denial laws (MacGuill 2017).

Other strategies for regulation exist. DiResta suggests that social media companies might be able to follow the example of numerous other industries and rebuild trust by creating a self-regulatory organization that establishes "industry-funded, industry-established voluntary-participation frameworks" (DiResta 2017). There are some grounds for skepticism of this approach, as Facebook has attempted to put the burden on individual advertisers by stating that "advertisers are responsible for understanding and complying with all applicable laws and regulations" (quoted in Thompson and Kulwin 2017). However, Twitter and Facebook have both recently introduced new features to show who bought advertisements, what advertisements were bought by a given page, and how the advertisements were targeted (Glaser 2017). Facebook proposed an "Election Integrity Initiative" that would improve transparency about advertising, and promote digital literacy and politicians' digital security (Canadian Press 2017).

Regardless of whether regulations are changed, countries and private companies need to improve their capacities to enforce regulations and respond to violations.

ABSENCE OF CLEAR INTERNATIONAL NORMS AND LAWS ON CYBER INTERFERENCE

There is a lack of clear international norms or laws regarding cyber-interference in elections, and therefore challenges in collective action to address the problem.

Cyber-interference has become a regular part of both "peacetime" state competition and as forms of "hybrid warfare" (Aro 2016; Gardener 2015; Pollock 2017).

In general, international law on cyber-operations (both hacking and information operations) is disputed, imprecise, and lacking in meaningful enforcement (Ohlin 2017).The *Tallinn Manual on Cyber Operations,* arguably the most influential guide on international law in this issue area, proposes that cyber violations of sovereignty require either a coercive intervention in the *domaine réservé* of a state, or the "interference or usurpation of inherently governmental functions" (Schmitt 2017, 20). However, information operations like those pursued by Russian in the US 2016 elections may not meet these criteria (Crootof 2018; Ohlin 2017). It is thus generally recognized that there are major gaps in international norms and laws to address such threats.

Relatedly, the longstanding international acceptance of espionage does not capture some risks that now exist. For instance, while espionage is generally not seen as a violation of *international* law, but rather as a possible violation of domestic law, digital technologies have enabled massive state-sponsored support for commercial spying and mass surveillance in other countries—generating calls for new international law paradigms to address them (Banks 2016; Finnemore and Hollis 2016). One approach may be to seek to enforce international human rights protections of privacy against surveillance and hacking by foreign states (Milanovic 2015).

Counter-measures

Scholars and practitioners have proposed modifications of international law in order to capture digital interference by foreign states. For instance, Crootof (2018) proposes a new category of international legal violation which she calls a "transnational cybertort," and which she distinguishes from cyberwar, cybercrime, and cyberespionage. While Crootof argues that responses to cybertorts could be pursued through existing international law, she suggests that it would be preferable to create a comprehensive international legal framework, and as well "a new, independent institution with the expertise and investigative resources to impartially assess state accountability in cyberspace" (64). In doing so, she joins many scholars, policymakers and stakeholders in seeking a new international regime. For instance, the president of Microsoft proposed the creation of a Digital Geneva Convention that would include clarify global cybersecurity rules and create an independent body – similar to the International Atomic Energy Agency – with the technical capacity to identify and monitor violations (Smith 2017). Along similar lines, prominent international law scholar, Duncan Hollis has suggested the need for "a global cyber federation, a federation of non-governmental institutions similar to the role that the Red Cross and Red Crescent movement," which would analyze and assist cyber attacks within states and across borders as needed (Hollis and Maurer 2015).

Other mechanisms currently exist to hold private foreign actors to account for violations of electoral law, or criminal law during elections. These include international cooperation on transnational prosecutions of cybercrime, including coordination via the Budapest Convention on Cybercrime (ratified by the US, Canada, most European states, and some other states). They also include fines against private businesses for violations of privacy, human rights, or other state regulations. In many of these cases, but particularly the prosecution of lone attackers, the difficult and cost of finding the responsible party,

extraditing an individual to Canada or launching a case in the appropriate jurisdiction, and then pursuing the case.

Another option for states is to threaten cyber-attacks in response to cyber interference. This is a new area of diplomacy and war, and expectations and risk calculations are uncertain. However, the particular dynamics of cyber operations – including the difficulty of attribution and the need for the particular mechanism of attack to remain secret – creates pressure for an escalation of system intrusion and counter-attacks (Buchanan 2017). While some scholars believe that devastating cyberwars may be unlikely (Gartzke 2013), most see political interference via information operations as an ongoing and escalating component of international conflict (Gardener 2015; Spruds et al. 2016).

Currently, however, there are no international policy levers to effectively address digital interference.

RESEARCH AND KNOWLEDGE GAPS

There are major knowledge deficits in this issue area. In particular, while there is a great deal of description of techniques used by foreign actors, there is little research showing their short-term or long-term impact, and almost no research on policy measures that might address these digital threats to democracy in Canada. Our review of the existing literature suggests more research is particularly needed on the following questions:

- What *normative frameworks* for democracy can suggest how contemporary media systems and DCTs might advance key democratic goods such as equal citizen participation, individual autonomy, sovereignty and self-determination, and robust, inclusive public deliberation?

- What impacts do the digital techniques described in this report have on *participation by individuals and groups* in democratic processes? Do trolling or misinformation operations affect the opinions and behaviour of people with different characteristics, such as differences on gender, education, age, political affiliation, or ethnicity?

- By what mechanisms can digital techniques significantly affect *electoral outcomes*? By "persuading" voters via misinformation and propaganda? By mobilizing or de-mobilizing people in key groups or constituencies to vote? By hacking attacks on voting machines? By unfairly supporting or harming particular candidates and parties?

- How are political parties, electoral commissions, and other democratic institutions affected by these digital techniques? How do they respond? Can cross-institutional comparisons reveal different vulnerabilities and effective counter-measures?

- Are there patterns to the use of digital techniques of electoral

interference by *different types of actors*, such as democratic or non-democratic states, corporations, transnational ideological or identity-based movements, cyber-criminals, and ideologically-committed individuals?

- Can *cross-national comparative analysis* reveal different vulnerabilities to digital techniques according to factors such as differing electoral systems, electoral regulations, national media systems, social media penetration, political polarization, or geopolitical alignments?

- What forms of social media platform design, public fact-checking, and digital literacy might *promote citizens' resistance* to misinformation and propaganda?

- What national and international *policy frameworks* can best address different types of digital interference by different types of foreign actors? What areas of regulation are most promising and challenging, from regulation of misinformation and hate on social media platforms, to criminal laws on hate or cyber-crimes, to electoral regulations on foreign interference and spending, to international laws against foreign interference?

CONCLUSION

The use of digital communication technologies to interfere in democracy, and elections in particular, is not new but is growing rapidly. While there has been great emphasis on the potential impact on electoral outcomes in the US and elsewhere, this report suggests that there are also profound threats to fair political participation, and that these threats may affect some groups disproportionately. There are also serious threats to trust, civility, truth-seeking, and ultimately to the legitimacy of democratic processes and institutions.

This report examines techniques of electoral interference that use DCTs, but it is not their technical dimensions alone that make them effective and dangerous. These techniques, and the actors who use them, leverage people's cognitive limitations, psychological predispositions and biases, political and cultural polarization, as well as deficits in media systems and democratic institutions. As a result, *solutions* to digital interference cannot simply be technical, nor can solutions be directed solely at foreign actors. Domestic actors in many countries also use these democracy-corroding digital techniques, and either knowingly or unknowingly augment the efforts of foreign actors to interfere with and undermine democratic processes.

A serious concern is that foreign and domestic actors, using digital and non-digital techniques, are creating *vicious circles* to undermine democracy. The effects of these techniques used by foreign actors – such as exacerbating social cleavages and distrust, or undermining fair participation and institutional effectiveness – can make democratic countries even more vulnerable to future interference. If such vicious circles continue, and the quality and legitimacy of democracy degrades, then it will become increasingly difficult for democratic states to advance their citizens' interests and resolve social conflicts.

Policymakers, citizens, and researchers therefore need to take serious and swift action. If they do so, many responses to foreign interference may also safeguard democracy from being degraded by domestic actors. And by improving the quality of democratic processes and institutions, we can help make our political systems more resistant to foreign interference. These *virtuous circles* should be what we aim for when we address digital threats to democracy.

WORKS CITED

Achen, Christopher H., and Larry M. Bartels. 2016. *Democracy for Realists: Why Elections Do Not Produce Responsive Government*. Princeton University Press.

Aiken, Mary. 2016. "Welcome to the Troll Election." *Time*. http://time.com/4371724/welcome-to-the-troll-election/ (December 28, 2017).

Albright, Jonathan. 2017. "Who Hacked the Election?" *Tow Center*. https://medium.com/tow-center/who-hacked-the-election-43d4019f705f (December 29, 2017).

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31(2): 211–36.

Anderson, Bruce, and David Coletto. 2017. "Canadian News Media And 'Fake News' Under A Microscope." *Abacus Data*. http://abacusdata.ca/canadian-news-media-and-fake-news-under-a-microscope/ (August 13, 2017).

Andress, Jason. 2011. *The Basics of Information Security*. Boston, MA: Syngress.

Anduiza, Eva, Michael James Jensen, and Laia Jorba, eds. 2012. *Digital Media and Political Engagement Worldwide: A Comparative Study*. Cambridge: Cambridge University Press.

Angwin, Julia. 2017. "Facebook's Secret Censorship Rules Protect White Men from Hate Speech But Not Black Children." *ProPublica*. https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms (June 30, 2017).

Angwin, Julia, Madeleine Varner, and Ariana Tobin. 2017. "Facebook Enabled Advertisers to Reach 'Jew Haters.'" *ProPublica*. https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters (November 16, 2017).

Applebaum, Anne. 2017. "Germany's Election Gives the Country a Reality Check." *The Washington Post*. https://www.washingtonpost.com/news/global-opinions/wp/2017/09/24/germanys-election-gives-the-country-a-reality-check/?utm_term=.c70bca162cd7 (December 13, 2017).

Aro, Jessikka. 2016. "The Cyberspace War: Propaganda and Trolling as Warfare Tools." *European View* 15(1): 121–32.

Baldwin-Philippi, Jessica. 2017. "The Myths of Data-Driven Campaigning." *Political Communication* 34(4): 627–33.

Banks, William C. 2016. "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage." *Emory Law Journal* 66: 513–25.

Bawn, Kathleen et al. 2012. "A Theory of Political Parties: Groups, Policy Demands and Nominations in American Politics." *Perspectives on Politics* 10(3): 571–97.

BBC. 2017. "Macron Leaks: The Anatomy of a Hack." *BBC News*. http://www.bbc.com/news/blogs-trending-39845105 (November 28, 2017).

Bell, Emily, and Taylor Owen. 2017. *The Platform Press: How Silicon Valley Reengineered Journalism*. New York: Tow Center for Digital Journalism, Columbia University.

Benkler, Yochai, Robert Faris, Hal Roberts, and Ethan Zuckerman. 2017. "Breitbart-Led Right-Wing Media Ecosystem Altered Broader Media Agenda." *Columbia Journalism Review*. https://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php (May 25, 2017).

Bennett, W. Lance, and Alexandra Segerberg. 2013. *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*. Cambridge: Cambridge University Press.

Berinsky, Adam J. 2017. "Rumors and Health Care Reform: Experiments in Political Misinformation." *British Journal of Political Science* 47(02): 241–62.

Berman, Russell. 2016. "What's the Answer to Political Polarization in the U.S.?" *The Atlantic*. https://www.theatlantic.com/politics/archive/2016/03/whats-the-answer-to-political-polarization/470163/ (July 12, 2017).

Bernstein, Joseph. 2017. "Here's How Breitbart And Milo Smuggled Nazi and White Nationalist Ideas Into The Mainstream." *BuzzFeed*. https://www.buzzfeed.com/josephbernstein/heres-how-breitbart-and-milo-smuggled-white-nationalism (October 23, 2017).

Bessi, Alessandro, and Emilio Ferrara. 2016. "Social Bots Distort the 2016 US Presidential Election Online Discussion." *First Monday* 21(11).

Bode, Leticia, and Emily K. Vraga. 2015. "In Related News, That Was Wrong: The Correction of Misinformation Through Related Stories Functionality in Social Media." *Journal of Communication* 65(4): 619–38.

———. 2017. "See Something, Say Something: Correction of Global Health Misinformation on Social Media." *Health Communication* 0(0): 1–10.

Bond, Robert M. et al. 2012. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489(7415): 295–98.

Bradshaw, Samantha, and Philip N Howard. 2017. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford, UK: Project on Computational Propaganda. Working Paper. http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/.

Brooks, Matt, Jakub Dalek, and Masashi Crete-Nishihata. 2016. "Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns." *The Citizen Lab*. https://citizenlab.ca/2016/04/between-hong-kong-and-burma/ (August 18, 2017).

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

Cadwalladr, Carole. 2017a. "'Dark Money' Is Threat to Integrity of UK Elections, Say Leading Academics." *The Guardian*. https://www.theguardian.com/politics/2017/apr/01/dark-money-threat-to-uk-elections-integrity (May 17, 2017).

———. 2017b. "The Great British Brexit Robbery: How Our Democracy Was Hijacked." *The Guardian*. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (May 9, 2017).

Calabresi, Massimo. 2017. "Election Hackers Altered Voter Rolls, Stole Private Data: Officials." *Time*. http://time.com/4828306/russian-hacking-election-widespread-private-data/ (August 2, 2017).

Cameron, Maxwell. 2013. *Strong Constitutions: Social-Cognitive Origins of the Separation of Powers*. Oxford: Oxford University Press.

Canadian Press. 2017. "Facebook to Use Canada as Testing Ground for New Ad Transparency Features." *CBC*. http://www.cbc.ca/news/business/facebook-test-ad-transparency-1.4376419 (November 29, 2017).

Canadian Security Intelligence Service. 2017. *Russian World-Views: Domestic Power Play and Foreign Behaviour*. Government of Canada.

Carlson, Matt. 2017. "Automating Judgment? Algorithmic Judgment, News Knowledge, and Journalistic Professionalism." *New Media & Society* 0(0): 1–18.

Carpini, Michael X. Delli, and Scott Keeter. 1996. *What Americans Know about Politics and Why It Matters*. New Haven, CT: Yale University Press.

Carvin, Stephanie, and Craig Forcese. 2017. "What Foreign Government Is in Your Stocking?" *A podcast Called INTREPID*. https://www.intrepidpodcast.com/podcast/2017/12/19/ep-16-what-foreign-government-is-in-your-stocking (December 20, 2017).

Chadwick, Andrew. 2006. *Internet Politics: States, Citizens, and New Communication Technologies*. Oxford: Oxford University Press.

Chadwick, Andrew, Ben O'Loughlin, and Cristian Vaccari. 2017. "Why People Dual Screen Political Debates and Why It Matters for Democratic Engagement." *Journal of Broadcasting & Electronic Media* 61(2): 220–39.

Chadwick, Andrew, and Jennifer Stromer-Galley. 2016. "Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?" *International Journal of Press/Politics*.

Chen, Liang, Shirley S Ho, and May O Lwin. 2017. "A Meta-Analysis of Factors Predicting Cyberbullying Perpetration and Victimization: From the Social Cognitive and Media Effects Approach." *New Media & Society* 19(8): 1194–1213.

Christl, Wolfie. 2017. "Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions." *Cracked Labs*. http://crackedlabs.org/en/corporate-surveillance (June 30, 2017).

Citizen Lab. n.d. "Security Planner: Home." *Security Planner*. https://securityplanner.org (December 29, 2017).

———. 2014. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. Toronto, ON: Citizen Lab, Munk School of Global Affairs, University of Toronto.

———. 2017. "Tainted Leaks: Disinformation and Phishing With a Russian Nexus." *The Citizen Lab*. https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/ (May 25, 2017).

Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press.

Clayton, Mark. 2014. "Ukraine Election Narrowly Avoided 'wanton Destruction' from Hackers." *Christian Science Monitor*. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers (October 5, 2017).

Coleman, Gabriella. 2017. "The Public Interest Hack." *Limn*. http://limn.it/the-public-interest-hack/ (May 17, 2017).

Collier, Kevin. 2017. "Prominent 'GOP' Twitter Account, Allegedly A Russian Troll, Was Widely Quoted In US Media." *BuzzFeed*. https://www.buzzfeed.com/kevincollier/americans-helped-spread-an-alleged-russian-gop-accounts (October 21, 2017).

Collins, Ben, Kevin Poulsen, and Spencer Ackerman. 2017. "Exclusive: Russians Impersonated Real American Muslims to Stir Chaos on Facebook and Instagram." *The Daily Beast*. http://www.thedailybeast.com/exclusive-russians-impersonated-real-american-muslims-to-stir-chaos-on-facebook-and-instagram (October 4, 2017).

Collins, Ben, Gideon Resnick, Kevin Poulsen, and Spencer Ackerman. 2017. "Exclusive: Russians Appear to Use Facebook to Push Trump Rallies in 17 U.S. Cities." *The Daily Beast*. http://www.thedailybeast.com/russians-appear-to-use-facebook-to-push-pro-trump-flash-mobs-in-florida (September 20, 2017).

Communications Security Establishment. 2017. *Cyber Threats to Canada's Democratic Process*. Government of Canada. https://www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf.

Craft, Stephanie, Seth Ashley, and Adam Maksl. 2017. "News Media Literacy and Conspiracy Theory Endorsement." *Communication and the Public* 2(4): 388–401.

Crootof, Rebecca. 2018. "Political Hacks: State Accountability in Cyberspace." *Cornell Law Review*. https://ssrn.com/abstract=2930700 (July 15, 2017).

Dahir, Abdi Latif, and Lily Kuo. 2017. "Kenya's Supreme Court Says the Presidential Election May Have Been Hacked." *Quartz*. https://qz.com/1082434/kenya-elections-kenyas-supreme-court-says-the-countrys-presidential-election-was-infiltrated-and-compromised/ (December 29, 2017).

Dahl, Robert A. 1989. *Democracy and Its Critics*. New Haven, CT: Yale University Press.

Dalton, Russell, and Martin Wattenberg. 2002. "Unthinkable Democracy: Political Change in Advanced Industrial Democracies." In *Parties without Partisans: Political Change in Advanced Industrial Democracies*, eds. Russell Dalton and Martin Wattenberg. Oxford: Oxford University Press, 3–18.

Deibert, Ronald. 2015. "Cyberspace Under Siege." *Journal of Democracy* 26(3): 64–78.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Del Vicario, Michela et al. 2016. "The Spreading of Misinformation Online." *Proceedings of the National Academy of Sciences* 113(3): 554–59.

Desigaud, Clementine et al. 2017. *Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?* Computational Propaganda Research Project, University of Oxford. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/05/What-Are-French-Voters-Sharing-Over-Twitter-Between-the-Two-Rounds-v9.pdf.

Devine, Curt. 2017. "'Kill Them All' -- Russian-Linked Facebook Accounts Called for Violence." *CNN*. http://money.cnn.com/2017/10/31/media/russia-facebook-violence/index.html (December 29, 2017).

Dewey, John. 1991. *The Public and Its Problems*. Athens: Swallow Press.

DFRLab. 2017. "Hashtag Campaign: #MacronLeaks." *DFRLab*. https://medium.com/dfrlab/hashtag-campaign-macronleaks-4a3fb870c4e8 (May 17, 2017).

Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21(3): 69–83.

Dickey, Christopher. 2017. "Did Macron Outsmart Campaign Hackers?" *The Daily Beast*. http://www.thedailybeast.com/did-macron-outsmart-campaign-hackers (June 29, 2017).

DiResta, Renee. 2017. "There Are Bots. Look Around." *ribbonfarm*. https://www.ribbonfarm.com/2017/05/23/there-are-bots-look-around/ (June 14, 2017).

Dixon-Woods, Mary et al. 2006. "Conducting a Critical Interpretive Synthesis of the Literature on Access to Healthcare by Vulnerable Groups." *BMC Medical Research Methodology* 6: 35–47.

Doman, Chris. 2017. "MacronLeaks – A Timeline of Events." *AlienVault*. https://www.alienvault.com/blogs/labs-research/macronleaks-a-timeline-of-events (August 2, 2017).

Donadio, Rachel. 2017. "Why the Macron Hacking Attack Landed With a Thud in France." *The New York Times*. https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html (May 9, 2017).

Doyle, Sady. 2017. "For the First Time, Death Threats Forced a Woman Out of a Congressional Race. It Won't Be the Last." *ELLE*. http://www.elle.com/culture/career-politics/news/a45762/kim-weaver-iowa-congressional-race-death-threats/ (October 10, 2017).

Druckman, James N., Erik Peterson, and Rune Slothuus. 2013. "How Elite Partisan Polarization Affects Public Opinion Formation." *American Political Science Review* 107(01): 57–79.

Drutman, Lee. 2017. "We Need New Ideas to Reduce Partisan Polarization." *Vox*. https://www.vox.com/polyarchy/2017/6/27/15880328/how-to-reduce-partisan-polarization (July 12, 2017).

Duncan, Jessica. 2016. "Russia Launches 'troll Factory' to Flood Internet with Lies about UK." *Mail Online*. http://www.dailymail.co.uk/~/article-3840816/index.html (August 26, 2017).

Earl, Jennifer, and Katrina Kimport. 2011. *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: MIT Press.

Elections Canada. "Election Advertising on the Internet." www.elections.ca/res/gui/app/2015-04/2015-04_e.pdf (November 2, 2017).

Elgot, Jessica, and Jamie Grierson. 2017. "Electoral Commission Launches Inquiry into Leave Campaign Funding." *The Guardian*. http://www.theguardian.com/politics/2017/nov/20/electoral-commission-launches-inquiry-into-leave-campaign-funding (January 2, 2018).

Eordogh, Fruzsina. 2016. "Pro-Trump Trolls Want You To Vote For Hillary Via Text (You Can't)." *Forbes*. https://www.forbes.com/sites/fruzsinaeordogh/2016/11/03/pro-trump-trolls-want-you-to-vote-for-hillary-via-text-you-cant/ (August 28, 2017).

Estlund, David M. 2009. *Democratic Authority: A Philosophical Framework*. Princeton, NJ: Princeton University Press.

Faris, Robert et al. 2017. *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*. Cambridge, MA: Berkman Klein Center for Internet & Society, Harvard University. SSRN Scholarly Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3019414 (October 6, 2017).

Ferrara, Emilio. 2017. "Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election." *First Monday* 22(8). http://firstmonday.org/ojs/index.php/fm/article/view/8005/6516 (August 23, 2017).

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110: 425–79.

Fitzgerald, Bill, and Kris Shaffer. 2017. "Spot a Bot: Identifying Automation and Disinformation on Social Media." *Medium*. https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203 (June 14, 2017).

Fonseca, Clotilde. 2010. "The Digital Divide and the Cognitive Divide: Reflections on the Challenge of Human Development in the Digital Age." *Information Technologies & International Development* 6(SE): 25–30.

Forestal, Jennifer. 2017. "The Architecture of Political Spaces: Trolls, Digital Media, and Deweyan Democracy." *American Political Science Review* 111(1): 149–61.

Franceschi-Bicchierai, Lorenzo. 2016. "Here's the Full Transcript of Our Interview With DNC Hacker 'Guccifer 2.0.'" *VICE: Motherboard*. https://motherboard.vice.com/en_us/article/yp3bbv/dnc-hacker-guccifer-20-full-interview-transcript (August 2, 2017).

Fredheim, Rolf, Alfred Moore, and John Naughton. 2015. "Anonymity and Online Commenting: The Broken Windows Effect and the End of Drive-by Commenting." In ACM Press, 1–8. http://dl.acm.org/citation.cfm?doid=2786451.2786459 (October 11, 2017).

Fuchs, Christian. 2017. *Social Media: A Critical Introduction*. 2nd ed. London: SAGE Publications.

Fung, Archon. 2013. "The Principle of Affected Interests: An Interpretation and Defense." In *Representation: Elections and Beyond*, eds. Jack H. Nagel and Rogers M. Smith. Philadelphia: University of Pennsylvania Press, 236–68.

Gardener, Hall. 2015. *Hybrid Warfare: Iranian and Russian Version of Little Green Men and Contemporary Conflict*. Rome: NATO Defense College.

Garofalo, Michael. 2016. "Trump's Frightening Internet Trolls: Online Harassment Has Become a Disturbing Tool for Many of His Supporters." *Salon*. http://www.salon.com/2016/03/14/the_donalds_frightening_internet_trolls_online_harassment_has_become_a_disturbing_tool_of_many_trump_supporters/ (August 28, 2017).

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38(2): 41–73.

Geybulla, Arzu. 2016. "In the Crosshairs of Azerbaijan's Patriotic Trolls." *openDemocracy*. https://www.opendemocracy.net/od-russia/arzu-geybulla/azerbaijan-patriotic-trolls (August 26, 2017).

Gillespie, Tarleton. 2010. "The Politics of 'Platforms.'" *New Media & Society* 12(3): 347–64.

Gilman, Nils, Jesse Goldhammer, and Steven Weber. 2017. "Can You Secure an Iron Cage?" *Limn*. https://limn.it/can-you-secure-an-iron-cage/ (June 30, 2017).

Glaser, April. 2017. "Political Ads on Facebook Now Need to Say Who Paid For Them." *Slate Magazine*. http://www.slate.com/blogs/future_tense/2017/12/18/political_ads_on_facebook_now_need_to_say_who_paid_for_them.html (January 2, 2018).

Goodin, Robert E. 1980. *Manipulatory Politics*. New Haven, CT: Yale University Press.

———. 2007. "Enfranchising All Affected Interests, and Its Alternatives." *Philosophy & Public Affairs* 35: 40–68.

Goodman, Ellen, and Lyndsey Wajert. 2017. *The Honest Ads Act Won't End Social Media Disinformation, but It's a Start*. Rutgers Law School. SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3064451 (January 3, 2018).

Gorton, William A. 2016. "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy." *New Political Science* 38(1): 61–80.

Grasseger, Hannes, and Mikael Krogerus. 2017. "The Data That Turned the World Upside Down." *Motherboard*. https://motherboard.vice.com/en_us/article/big-data-cambridge-analytica-brexit-trump (May 17, 2017).

Greenberg, Andy. 2017. "How An Entire Nation Became Russia's Test Lab for Cyberwar." *WIRED*. https://www.wired.com/story/russian-hackers-attack-ukraine/ (June 30, 2017).

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Macmillan.

grugq, the. 2017. "American Snoper." *the grugq*. https://medium.com/@thegrugq/american-sniper-6d28e833b377 (May 17, 2017).

Gu, Lion, Vladimir Kropotov, and Fyodor Yarochkin. 2017. *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*. TrendMicro. https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf.

Guardian Staff. 2017. "Cyber-Attack on Parliament Leaves MPs Unable to Access Emails." *The Guardian*. https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access (June 26, 2017).

Guess, Andrew, Brendan Nyhan, and Jason Reifler. 2018. *Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign.*. SSRN Scholarly Paper. https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf (January 1, 2018).

Gunitsky, Seva. 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13(1): 42–54.

Habermas, Jürgen. 1990. *Moral Consciousness and Communicative Action*. Cambridge, MA: MIT Press.

———. 1991. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: MIT Press.

Hacker, Jacob S., and Paul Pierson. 2015. "Confronting Asymmetric Polarization." In *Solutions to Political Polarization in America*, ed. Nathaniel Persily. Cambridge: Cambridge University Press.

Hague, Barry N., and Brian Loader, eds. 1999. *Digital Democracy: Discourse and Decision Making in the Information Age*. London: Routledge.

von Hammerstein, Konstantin, Roman Höfner, and Marcel Rosenbach. 2017. "March of the Trolls: Right-Wing Activists Take Aim at German Election." *Spiegel Online*. http://www.spiegel.de/international/germany/trolls-in-germany-right-wing-extremists-stir-internet-hate-a-1166778.html (December 20, 2017).

Hanitzsch, Thomas, Arjen Van Dalen, and Nina Steindl. 2018. "Caught in the Nexus: A Comparative and Longitudinal Analysis of Public Trust in the Press." *The International Journal of Press/Politics* 23(1): 3–23.

Hannan, Jason. 2017. "Trolling Ourselves to Death in the Age of Trump." *The Conversation*. http://theconversation.com/trolling-ourselves-to-death-in-the-age-of-trump-80524 (August 26, 2017).

Hardaker, Claire. 2010. "Trolling in Asynchronous Computer-Mediated Communication: From User Discussions to Academic Definitions." *Journal of Politeness Research: Language, Behavior, Culture* 6(2): 215–42.

Hare, Stephanie. 2016. "For Your Eyes Only: U.S. Technology Companies, Sovereign States, and the Battle over Data Protection." *Business Horizons* 59(5): 549–61.

Henrichsen, Jenn. 2015. "The Dangers of Journalism Include Getting Doxxed. Here's What You Can Do about It." *Poynter*. https://www.poynter.org/2015/the-dangers-of-journalism-include-getting-doxxed-heres-what-you-can-do-about-it/345449/ (August 26, 2017).

Hern, Alex. 2016. "Facebook, YouTube, Twitter and Microsoft Sign EU Hate Speech Code." *The Guardian*. http://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code (January 3, 2018).

Herring, Susan, Kirk Job-Sluder, Rebecca Scheckler, and Sasha Barab. 2011. "Searching for Safety Online: Managing 'Trolling' in a Feminist Forum." *The Information Society* 18(5): 371–84.

Hersh, Eitan. 2015. *Hacking the Electorate: How Campaigns Perceive Voters*. Cambridge: Cambridge University Press.

Hjelmgaard, Kim. 2017. "There Is Meddling in Germany's Election — Not by Russia, but by U.S. Right Wing." *USA TODAY*. https://www.usatoday.com/story/news/world/2017/09/20/meddling-germany-election-not-russia-but-u-s-right-wing/676142001/ (December 28, 2017).

Hollis, Duncan, and Tim Maurer. 2015. "A Red Cross for Cyberspace." *TIME*. http://time.com/3713226/red-cross-cyberspace/ (November 21, 2017).

Holtz-Bacha, Christina, Marion R. Just, Travis Ridout, and Jenny L. Holland, eds. 2017. "The Effects of Political Advertising." In *Routledge Handbook of Political Advertising*, New York: Routledge, 61–71.

Howard, Philip N et al. 2017. *Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter in Round Two?* Computational Propaganda Research Project, University of Oxford. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/04/What-Are-French-Voters-Sharing-Over-Twitter-v10.pdf.

Howard, Philip N, and Muzammil M Hussain. 2013. *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. Oxford: Oxford University Press.

IISP. 2016. *The State of the Profession: Security Market Trends and Predictions*. Institute of Information Security Professionals. https://www.iisp.org/imis15/iisp/About_Us/IISP_Media/iispv2/About_us/IISP.aspx?hkey=866b64e2-77f2-4159-9acd-134c01ae54cf.

Illing, Sean. 2017. "Cambridge Analytica, the Shady Data Firm That Might Be a Key Trump-Russia Link, Explained." *Vox*. https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-trump-kushner-flynn-russia (October 23, 2017).

Invernizzi-Accetti, Carlo, and Fabio Wolkenstein. 2017. "The Crisis of Party Democracy, Cognitive Mobilization, and the Case for Making Parties More Deliberative." *American Political Science Review* 111(01): 97–109.

Isaac, Mike, and Scott Shane. 2017. "Facebook's Russia-Linked Ads Came in Many Disguises." *The New York Times*. https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html (October 5, 2017).

Isaac, Mike, and Daisuke Wakabayashi. 2017. "Russian Influence Reached 126 Million Through Facebook Alone." *The New York Times*. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html (November 20, 2017).

Iyengar, Shanto, and Sean J. Westwood. 2015. "Fear and Loathing across Party Lines: New Evidence on Group Polarization." *American Journal of Political Science* 59(3): 690–707.

Jack, Caroline. 2017. "Lexicon of Lies: Terms for Problematic Information." https://datasociety.net/output/lexicon-of-lies/ (September 15, 2017).

Jarvis, Jeff. 2017. "Our Problem Isn't 'Fake News.' Our Problems Are Trust and Manipulation." *Medium*. https://medium.com/whither-news/our-problem-isnt-fake-news-our-problems-are-trust-and-manipulation-5bfbcd716440 (June 21, 2017).

Kahan, Dan. 2013. "Ideology, Motivated Reasoning, and Cognitive Reflection." *Judgment and Decision Making* 8(4): 407–24.

Kahne, Joseph, and Benjamin Bowyer. 2017. "Educating for Democracy in a Partisan Age: Confronting the Challenges of Motivated Reasoning and Misinformation." *American Educational Research Journal* 54(1): 3–34.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kalla, Joshua L., and David E. Broockman. 2017. "The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments." *American Political Science Review*: 1–19.

Karpf, David. 2012. *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy*. Oxford: Oxford University Press.

King, Esther. 2016. "Russian Hackers Targeting Germany: Intelligence Chief." *Politico EU*. http://www.politico.eu/article/german-intelligence-chief-russian-hackers-targeting-us-bruno-kahl-vladimir-putin/ (September 15, 2017).

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111(3): 484–501.

Kinstler, Linda. 2017. "Can Germany Fix Facebook?" *The Atlantic*. https://www.theatlantic.com/international/archive/2017/11/germany-facebook/543258/ (November 8, 2017).

Klobuchar, Amy. 2017. "S.1989 - 115th Congress (2017-2018): Honest Ads Act." https://www.congress.gov/bill/115th-congress/senate-bill/1989 (December 13, 2017).

Kopan, Tal. 2017. "DHS Offcials: 21 States Potentially Targeted by Russia Hackers Pre-Election." *CNN*. http://www.cnn.com/2017/06/21/politics/russia- hacking-hearing-states-targeted/index.htm (October 30, 2017).

Kosinski, Michal, and Yilun Wang. forthcoming. "Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images." *Journal of Personality and Social Psychology*. https://osf.io/zn79k/ (October 5, 2017).

Kreiss, Daniel. 2016. *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. Oxford: Oxford University Press.

Kreiss, Daniel, Regina G. Lawrence, and Shannon C. McGregor. 2017. "In Their Own Words: Political Practitioner Accounts of Candidates, Audiences, Affordances, Genres, and Timing in Strategic Social Media Use." *Political Communication*: 1–24.

Krupnikov, Yanna. 2014. "How Negativity Can Increase and Decrease Voter Turnout: The Effect of Timing." *Political Communication* 31(3): 446–66.

Kuklinski, James H. et al. 2000. "Misinformation and the Currency of Democratic Citizenship." *The Journal of Politics* 62(3): 790–816.

Lapowsky, Issie. 2017. "The Real Trouble With Trump's 'Dark Post' Facebook Ads." *WIRED*. https://www.wired.com/story/trump-dark-post-facebook-ads/ (October 17, 2017).

Lazer, David et al. 2017. "Combating Fake News: An Agenda for Research and Action." *Shorenstein Center*. https://shorensteincenter.org/combating-fake-news-agenda-for-research/ (May 25, 2017).

Lee, Bryan. 2016. "The Impact of Cyber Capabilities in the Syrian Civil War." *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war (August 25, 2017).

Legum, Judd. 2017. "Trump Mentioned Wikileaks 164 Times in Last Month of Election, Now Claims It Didn't Impact One Voter." *ThinkProgress*. https://thinkprogress.org/trump-mentioned-wikileaks-164-times-in-last-month-of-election-now-claims-it-didnt-impact-one-40aa62ea5002/ (August 26, 2017).

Levendusky, Matthew S. 2013. "Why Do Partisan Media Polarize Viewers?" *American Journal of Political Science* 57(3): 611–23.

Levin, Dov H. 2016. "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results." *International Studies Quarterly* 60(2): 189–202.

Lewis, Alan, and Dan McKone. 2016. "To Get More Value from Your Data, Sell It." *Harvard Business Review*. https://hbr.org/2016/10/to-get-more-value-from-your-data-sell-it (October 23, 2017).

Lipton, Eric, and David E. Sanger. 2016. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *New York Times*. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Lister, Tim, and Clare Sebastian. 2017. "Stoking Islamophobia and Secession in Texas -- from an Office in Russia." *CNN*. http://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html (December 28, 2017).

Lubben, Alex. 2017. "This One Insane Day Changed the Course of U.S. Politics Forever." *Vice News*. https://news.vice.com/story/this-one-insane-day-changed-the-course-of-u-s-politics-forever (August 2, 2017).

Lynch, Marc, Deen Freelon, and Sean Aday. 2016. *How Social Media Undermines Transitions to Democracy*. Washington, DC: PeaceTech Lab.

Lyons, Benjamin. 2017a. "Insidiously Trivial: How Political Memes Drive Down Corrective Intent." University of Exeter. Working Paper. https://www.academia.edu/33740160/Insidiously_Trivial_How_Political_Memes_Drive_Down_Corrective_Intent.

———. 2017b. "When Readers Believe Journalists: Effects of Adjudication in Varied Dispute Contexts." *International Journal of Public Opinion Research* 0(0).

MacGuill, Dan. 2017. "Does Setting Your Twitter Location to Germany Block Nazi Content?" *Snopes*. https://www.snopes.com/twitter-germany-nazis/.

Maksl, Adam, Stephanie Craft, Seth Ashley, and Dean Miller. 2017. "The Usefulness of a News Media Literacy Measure in Evaluating a News Literacy Curriculum." *Journalism & Mass Communication Educator* 72(2): 228–41.

Manjoo, Farhad. 2017. "How Twitter Is Being Gamed to Feed Misinformation." *The New York Times*. https://www.nytimes.com/2017/05/31/technology/how-twitter-is-being-gamed-to-feed-misinformation.html (June 14, 2017).

Mansbridge, Jane et al. 2012. "A Systemic Approach to Deliberative Democracy." In *Deliberative Systems: Deliberative Democracy at the Large Scale*, Cambridge: Cambridge University Press, 1–26.

Mantilla, Karla. 2015. *Gendertrolling: How Misogyny Went Viral*. Santa Barbara, California: Praeger.

Margetts, Helen. 2017. "Political Behaviour and the Acoustics of Social Media." *Nature Human Behaviour* 1. https://www.readcube.com/articles/10.1038/s41562-017-0086 (September 20, 2017).

Margetts, Helen, Peter John, Scott Hale, and Taha Yasseri. 2015. *Political Turbulence: How Social Media Shape Collective Action*. Princeton, NJ: Princeton University Press.

Margolis, Michael, and Gerson Moreno-Riaño. 2009. *The Prospect of Internet Democracy*. Burlington, VA: Ashgate.

Martin, Jonathan. 2017. "Dubious Vote-Fraud Claim Gets the Trump Seal of Approval." *The New York Times*. https://www.nytimes.com/2017/01/27/us/politics/donald-trump-voter-fraud.html (July 11, 2017).

Marwick, Alice, and Rebecca Lewis. 2017. *Media Manipulation and Disinformation Online*. New York: Data & Society Research Institute. https://datasociety.net/output/media-manipulation-and-disinfo-online/ (May 17, 2017).

Massanari, Adrienne. 2017. "#Gamergate and The Fappening: How Reddit's Algorithm, Governance, and Culture Support Toxic Technocultures." *New Media & Society* 19(3): 329–46.

Matias, J. Nathan. 2017. "The Real Name Fallacy." *The Coral Project*. https://blog.coralproject.net/the-real-name-fallacy/ (November 20, 2017).

McKelvey, Fenwick, and Elizabeth Dubois. 2017. *Computational Propaganda in Canada*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Canada.pdf.

Messing, Solomon, and Sean J. Westwood. 2014. "Selective Exposure in the Age of Social Media: Endorsements Trump Partisan Source Affiliation When Selecting News Online." *Communication Research* 41(8): 1042–63.

Milanovic, Marko. 2015. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harvard International Law Journal* 56: 81–146.

Monaco, Nicholas J. 2017. *Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy*. Computational Propaganda Research Project, University of Oxford. Working Paper.

Morell, Michael, and Suzanne Kelly. 2016. "Fmr. CIA Acting Dir. Michael Morell: 'This Is the Political Equivalent of 9/11.'" *The Cipher Brief*. https://www.thecipherbrief.com/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091 (August 13, 2017).

Morgan, Jonathon, and Kris Shaffer. 2017. "Sockpuppets, Secessionists, and Breitbart." *Data for Democracy*. https://medium.com/data-for-democracy/sockpuppets-secessionists-and-breitbart-7171b1134cd5 (June 14, 2017).

Nagle, Angela. 2017. *Kill All Normies: Online Culture Wars From 4Chan And Tumblr To Trump And The Alt-Right*. Winchester, UK: Zero Books.

Nakashima, Ellen. 2017. "Israel Hacked Kaspersky, Then Tipped the NSA That Its Tools Had Been Breached." *Washington Post*. https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html? (October 14, 2017).

National Election Defense Coalition. 2017. "Election Integrity Expert Letter to Congress." *Election Defense*. https://www.electiondefense.org/election-integrity-expert-letter/ (August 23, 2017).

Nelson, Jacob L., and James G. Webster. 2017. "The Myth of Partisan Selective Exposure: A Portrait of the Online Political News Audience." *Social Media + Society* 3(3): 1–13.

Neudert, Lisa-Maria N. 2017. *Computational Propaganda in Germany: A Cautionary Tale*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Germany.pdf.

Norden, Lawrence, and Ian Vandewalker. 2017. *Securing Elections From Foreign Interference*. Brennan Center for Justice, NYU School of Law. https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_0.pdf.

Norden, Lawrence, Ian Vandewalker, and Meg Charlton. 2017. "This Bill Would Help Stop Russia From Buying Online Election Ads." *Slate*. http://www.slate.com/articles/technology/future_tense/2017/10/the_honest_ads_act_would_help_stop_online_election_meddling_from_foreign.html (January 3, 2018).

Nyhan, Brendan, and Yusaku Horiuchi. 2017. "Homegrown 'Fake News' Is a Bigger Problem than Russian Propaganda. Here's a Way to Make Falsehoods More Costly for Politicians." *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/10/23/homegrown-fake-news-is-a-bigger-problem-than-russian-propaganda-heres-a-way-to-make-falsehoods-more-costly-for-politicians/ (December 3, 2017).

Nyhan, Brendan, and Jason Reifler. 2016. "Do People Actually Learn From Fact-Checking? Evidence from a Longitudinal Study during the 2014 Campaign." *Working paper*. http://www.dartmouth.edu/~nyhan/fact-checking-effects.pdf (March 20, 2017).

O'Carroll, Tanya, and Alberto Escorcia. 2017. "Mexico's Misinformation Wars: How Organized Troll Networks Attack and Harass Journalists and Activists in Mexico." *OpenDemocracy*. https://www.opendemocracy.net/hri/tanya-ocarroll/mexicos-misinformation-wars (August 22, 2017).

Office of Director of National Intelligence. 2017. "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections." https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ohlin, Jens David. 2017. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95(7): 1579–98.

Olmstead, Kenneth, and Aaron Smith. 2017. "Americans and Cybersecurity." *Pew Research Center: Internet, Science & Tech*. http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ (October 23, 2017).

Ong, Thuy. 2017. "Facebook Found a Better Way to Fight Fake News." *The Verge*. https://www.theverge.com/2017/12/21/16804912/facebook-disputed-flags-misinformation-news-feed-fake-news (January 2, 2018).

Owen, Taylor. 2015. *Disruptive Power: Digital Technology and the Remaking of International Affairs*. Oxford: Oxford University Press.

Pao, Ellen. 2015. "Former Reddit CEO Ellen Pao: The Trolls Are Winning the Battle for the Internet." *The Washington Post*.

Pariser, Eli. 2011. *The Filter Bubble: What The Internet Is Hiding From You*. New York: Penguin Books Limited.

Parsons, Christopher. 2015. "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance." *Media and Communication* 3: 1–11.

Paul, Christopher, and Miriam Matthews. 2016. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." *RAND Corporation*. https://www.rand.org/pubs/perspectives/PE198.html (December 29, 2017).

Pennycook, Gordon, and David G. Rand. 2017a. *Assessing the Effect of "Disputed" Warnings and Source Salience on Perceptions of Fake News Accuracy*. . SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3035384 (September 25, 2017).

———. 2017b. *Who Falls for Fake News? The Roles of Analytic Thinking, Motivated Reasoning, Political Ideology, and Bullshit Receptivity*. . SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3023545 (September 8, 2017).

Perlroth, Nicole, Michael Wines, and Matthew Rosenberg. 2017. "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny." *The New York Times*. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html (September 15, 2017).

Persily, Nathaniel. 2017. "Can Democracy Survive the Internet?" *Journal of Democracy* 28(2): 63–76.

Perski, Olga, Ann Blandford, Robert West, and Susan Michie. 2017. "Conceptualising Engagement with Digital Behaviour Change Interventions: A Systematic Review Using Principles from Critical Interpretive Synthesis." *Translational Behavioral Medicine* 7(2): 254–67.

Peters, Jeremy W. 2017. "A Pro-Trump Conspiracy Theorist, a False Tweet and a Runaway Story." *The New York Times*. https://www.nytimes.com/2017/06/10/us/politics/comey-fake-news-twitter-posobiec.html (June 14, 2017).

Peterson, Andrea. 2016. "Wikileaks Posts Nearly 20,000 Hacked DNC Emails Online." *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2016/07/22/wikileaks-posts-nearly-20000-hacked-dnc-emails-online/ (July 3, 2017).

Phillips, Whitney. 2015. *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*. Cambridge, MA: MIT Press.

Pollock, John. 2017. "Russian Disinformation Technology." *MIT Technology Review*. https://www.technologyreview.com/s/604084/russian-disinformation-technology/ (June 29, 2017).

Privacy International. 2016. "New Court Judgment Finds UK Surveillance Agencies Collected Everyone's Communications Data Unlawfully and in Secret, for over a Decade." *Privacy International*. https://www.privacyinternational.org/node/938.

Przeworski, Adam. 1999. "Minimalist Conception of Democracy: A Defense." In *Democracy's Values*, eds. Ian Shapiro and Casiano Hacker-Cordón. Cambridge: Cambridge University Press, 23–55.

Rainie, Lee, Janna Anderson, and Jonathan Albright. 2017. "The Future of Free Speech, Trolls, Anonymity and Fake News Online." *Pew Research Center*. http://www.pewinternet.org/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/ (August 28, 2017).

Rid, Thomas. 2016. "The Plot Against America Part 1: How Russia Pulled Off the Biggest Election Hack in U.S. History." *Esquire* 166: 130–53.

Roberts, Sarah T. 2017. "Social Media's Silent Filter." *The Atlantic*. https://www.theatlantic.com/technology/archive/2017/03/commercial-content-moderation/518796/ (January 2, 2018).

Robertson, Jordan, Michael Riley, and Andrew Willis. 2016. "How to Hack an Election." *Bloomberg Businessweek*. https://www.bloomberg.com/features/2016-how-to-hack-an-election/.

Rojecki, Andrew, and Sharon Meraz. 2016. "Rumors and Factitious Informational Blends: The Role of the Web in Speculative Politics." *New Media & Society* 18(1): 25–43.

Roy, Jeffrey. 2016. "Secrecy, Security and Digital Literacy in an Era of Meta-Data: Why the Canadian Westminster Model Falls Short." *Intelligence and National Security* 31(1): 95–117.

Sanovich, Sergey. 2017. *Computational Propaganda in Russia: The Origins of Digital Disinformation*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf.

Sauter, Molly. 2017. "The Illicit Aura of Information." *Limn*. https://limn.it/the-illicit-aura-of-information/ (May 17, 2017).

Savage, Charlie. 2016. "Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention." *The New York Times*. https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html (August 2, 2017).

Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Scott, Mark. 2017. "U.S. Far-Right Activists Promote Hacking Attack Against Macron." *The New York Times*. https://www.nytimes.com/2017/05/06/world/europe/emmanuel-macron-hack-french-election-marine-le-pen.html (May 9, 2017).

Segal, Adam. 2017. "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" *Council on Foreign Relations*. https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what (October 5, 2017).

Sen, Amartya. 2009. *The Idea of Justice*. Cambridge, MA: Belknap Press.

Shackelford, Scott et al. 2017. "Making Democracy Harder to Hack." *University of Michigan Journal of Law Reform* 50(3): 629–68.

Shao, C., G.L. Ciampaglia, A. Flammini, and F Menczer. 2016. "Hoaxy: A Platform for Tracking Online Misinformation." https://arxiv.org/abs/1603.01511.

Shao, Chengcheng et al. 2017. "The Spread of Fake News by Social Bots." *arXiv:1707.07592*. https://scirate.com/arxiv/1707.07592 (July 25, 2017).

Shearlaw, Maeve. 2016. "Turkish Journalists Face Abuse and Threats Online as Trolls Step up Attacks." *The Guardian*. https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-threats-online-trolls-attacks (August 26, 2017).

Silverman, Craig. 2016. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook." *Buzzfeed*. https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook? (August 8, 2017).

Silverman, Craig, Jane Lytvynenko, Lam Thoy Vo, and Jeremy Singer-Vine. 2017. "Inside The Partisan Political Fight For Your Facebook News Feed." *BuzzFeed*. https://www.buzzfeed.com/craig-silverman/inside-the-partisan-fight-for-your-news-feed (August 8, 2017).

Sloane, Garett. 2017. "'We're Not Dumb': Brands Worry Twitter Underestimates Its Bot Problem." http://adage.com/article/digital/brands-worry-twitter-underestimates-impact-bots-ads/309665/ (July 19, 2017).

Smith, Brad. 2017. "The Need for a Digital Geneva Convention." *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (May 17, 2017).

Smyrnaios, Nikos, Sophie Chauvet, and Emmanuel Marty. 2017. *The Impact of CrossCheck on Journalists & the Audience*. Cambridge, MA: First Draft News, Shorenstein Center on Media, Politics and Public Policy, Harvard University. https://firstdraftnews.com/wp-content/uploads/2017/11/crosscheck_qual_EN.pdf/ (November 20, 2017).

Sollenberger, Roger. 2017. "How the Trump-Russia Data Machine Games Google to Fool Americans." *Paste Magazine*. https://www.pastemagazine.com/articles/2017/06/how-the-trump-russia-data-machine-games-google-to.html (June 14, 2017).

Spike, Carlett, and Pete Vernon. 2017. "'It Was Super Graphic': Reporters Reveal Stories of Online Harassment." *Columbia Journalism Review*. https://www.cjr.org/covering_trump/journalists-harassment-trump.php (December 28, 2017).

Spruds, Andris et al. 2016. *Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia*. Riga, Latvia: NATO Strategic Communication Centre of Excellence. http://www.stratcomcoe.org/download/file/fid/3353.

Stamos, Alex. 2017. "An Update On Information Operations On Facebook." *Facebook Newsroom*. https://newsroom.fb.com/news/2017/09/information-operations-update/ (September 20, 2017).

Standing Senate Committee on Legal and Constitutional Affairs. 2017. *Controlling Foreign Influence in Canadian Elections*. Ottawa: Senate of Canada.

Stanford History Education Group. 2016. *Evaluating Information: The Cornerstone of Civic Online Reasoning*. Stanford University: Stanford. https://purl.stanford.edu/fv751yt5934.

Starbird, Kate. 2017. "Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter." *ICWSM*: 230–39.

Stecula, Dominik. 2017. "Fake News Might Be Harder to Spot than Most People Believe." *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/10/fake-news-might-be-harder-to-spot-than-most-people-believe/?utm_term=.3bab9c87b0f1 (July 10, 2017).

Stelzenmüller, Constanze. 2017. "The Impact of Russian Interference on Germany's 2017 Elections." *Brookings*. https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/ (August 27, 2017).

Subramanian, Samanth. 2017. "Meet the Macedonian Teens Who Mastered Fake News and Corrupted the US Election." *WIRED*. https://www.wired.com/2017/02/veles-macedonia-fake-news/ (July 12, 2017).

Sullivan, Mark. 2017. "FEC Gets Over 150,000 Comments About Online Political Ad Disclaimers." *Fast Company*. https://www.fastcompany.com/40495435/fec-gets-over-150000-comments-about-online-political-ads-transparency (January 2, 2018).

Tambini, Darian, Sharif Labo, Emma Goodman, and Martin Moore. 2017. *The New Political Campaigning*. London: Media Policy Project, London School of Economics and Political Science. http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-%20The%20new%20political%20campaigning_final.pdf.

Teachout, Zephyr. 2009. "Extraterritorial Electioneering and the Globalization of American Elections." *Berkeley Journal of International Law* 27: 162–91.

Tenove, Chris, Andrés Delgado, and John Woodside. 2016. "With Authoritarianism and State Surveillance on the Rise, How Can Civil Society Be Protected from Digital Threats?" *OpenCanada*. https://www.opencanada.org/features/authoritarianism-and-state-surveillance-rise-how-can-civil-society-be-protected-digital-threats/ (November 20, 2017).

Thomas, Kurt et al. 2013. "Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse." In *Proceedings of the 22nd USENIX Security Symposium*, Washington, D.C.

Thompson, Alex, and Noah Kulwin. 2017. "No One Is Tracking the Illegal Political Ads in Your Facebook Feed." *VICE News*. https://news.vice.com/en_us/article/595k78/facebook-political-ads (January 2, 2018).

Timberg, Craig. 2017. "Russian Propaganda May Have Been Shared Hundreds of Millions of Times, New Research Says." *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says/ (October 10, 2017).

Tobin, Ariana, Madeleine Varner, and Julia Angwin. 2017. "Facebook's Uneven Enforcement of Hate Speech Rules...." *ProPublica*. https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes (January 2, 2018).

Tsagourias, N. 2016. "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts." *Journal of Conflict and Security Law* 21: 455–74.

Tsagourias, Nicholas. 2015. "The Legal Status of Cyberspace." In *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan. Cheltenham, UK: Edward Elgar Publishing Limited, 13–29.

Twitter. 2017. "Announcement: RT and Sputnik Advertising." *Blog.Twitter*. https://blog.twitter.com/official/en_us/topics/company/2017/Announcement-RT-and-Sputnik-Advertising.html (November 17, 2017).

Tworek, Heidi. 2017a. "Cambridge Analytica, Trump, and the New Old Fear of Manipulating the Masses." *Nieman Lab*. http://www.niemanlab.org/2017/05/cambridge-analytica-trump-and-the-new-old-fear-of-manipulating-the-masses/ (October 5, 2017).

———. 2017b. "How Germany Is Tackling Hate Speech." *Foreign Affairs*. https://www.foreignaffairs.com/articles/germany/2017-05-16/how-germany-tackling-hate-speech (November 3, 2017).

United Nations General Assembly. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."

Vaccari, Cristian. 2013. *Digital Politics in Western Democracies: A Comparative Study*. Baltimore, MD: Johns Hopkins University Press.

Vargo, Chris J, Lei Guo, and Michelle A Amazeen. 2017. "The Agenda-Setting Power of Fake News: A Big Data Analysis of the Online Media Landscape from 2014 to 2016." *New Media & Society* 0(0).

Vijayan, Jaikumar. 2015. "The Identity Underworld: How Criminals Sell Your Data on the Dark Web." *Christian Science Monitor*. https://www.csmonitor.com/World/Passcode/2015/0506/The-identity-underworld-How-criminals-sell-your-data-on-the-Dark-Web (October 23, 2017).

Wakefield, Jane. 2017. "Facebook's Fake News Experiment Backfires." *BBC News*. http://www.bbc.com/news/technology-41900877 (November 17, 2017).

Wardle, Claire, and Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe. https://firstdraftnews.com/wp-content/uploads/2017/10/Information_Disorder_FirstDraft-CoE_2018.pdf?x56713.

Warren, Mark E. 1999. *Democracy and Trust*. Cambridge: Cambridge University Press.

———. 2017. "A Problem-Based Approach to Democratic Theory." *American Political Science Review* 111(1): 39–53.

Weeks, Brian E., and R. Kelly Garrett. 2014. "Electoral Consequences of Political Rumors: Motivated Reasoning, Candidate Rumors, and Vote Choice during the 2008 U.S. Presidential Election." *International Journal of Public Opinion Research* 26(4): 401–22.

Weeks, Brian, and Brian Southwell. 2010. "The Symbiosis of News Coverage and Aggregate Online Search Behavior: Obama, Rumors, and Presidential Politics." *Mass Communication and Society* 13(4): 341–60.

West, Darrell M. 2017. "How to Combat Fake News and Disinformation." *The Brookings Institution*. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/ (December 30, 2017).

Willsher, Kim. 2017. "French Media Warned Not to Publish Emmanuel Macron Leaks." *The Observer*. http://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks (August 3, 2017).

Wingfield, Nick, Mike Isaac, and Katie Benner. 2016. "Google and Facebook Take Aim at Fake News Sites." *The New York Times*. https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html (September 25, 2017).

Wood, Thomas, and Ethan Porter. 2016. *The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence*. . SSRN Scholarly Paper. https://papers.ssrn.com/abstract=2819073 (May 3, 2017).

Woolley, Samuel C., and Douglas R. Guilbeault. 2017. *Computational Propaganda in the United States of America: Manufacturing Consensus Online*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf.

Woolley, Samuel C., and Philip N Howard. 2017. *Computational Propaganda Worldwide: Executive Summary*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Wright, Scott, and John Street. 2007. "Democracy, Deliberation and Design: The Case of Online Discussion Forums." *New Media & Society* 9(5): 849–69.

Yeung, Karen. 2017. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 0(0).

Young, Iris Marion. 2000. *Inclusion and Democracy*. Oxford: Oxford University Press.

Zhdanova, Mariia, and Dariya Orlova. 2017. *Computational Propaganda in Ukraine: Caught between External Threats and Internal Challenges*. Computational Propaganda Research Project, University of Oxford. Working Paper. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf.